S. HRG. 99-536

COMPUTER PORNOGRAPHY AND CHILD EXPLOITATION PREVENTION ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON JUVENILE JUSTICE

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

NINETY-NINTH CONGRESS

FIRST SESSION

ON

S. 1305

A BILL TO AMEND TITLE 18, UNITED STATES CODE, TO ESTABLISH CRIMINAL PENALTIES FOR THE TRANSMISSION BY COMPUTER OF OBSCENE MATTER, OR BY COMPUTER OR OTHER MEANS, OF MATTER PERTAINING TO THE SEXUAL EXPLOITATION OF CHILDREN, AND FOR OTHER PURPOSES

OCTOBER 1, 1985

Serial No. J-99-59

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

56-908 O WASHINGTON : 1986

S521-48

COMMITTEE ON THE JUDICIARY

STROM THURMOND, South Carolina, *Chairman*

CHARLES McC. MATHIAS, JR., Maryland
PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah
ALAN K. SIMPSON, Wyoming
JOHN P. EAST, North Carolina
CHARLES E. GRASSLEY, Iowa
JEREMIAH DENTON, Alabama
ARLEN SPECTER, Pennsylvania
MITCH McCONNELL, Kentucky

JOSEPH R. BIDEN, JR., Delaware
EDWARD M. KENNEDY, Massachusetts
ROBERT C. BYRD, West Virginia
HOWARD M. METZENBAUM, Ohio
DENNIS DECONCINI, Arizona
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois

DENNIS W. SHEDD, *Chief Counsel and Staff Director*
DIANA L. WATERMAN, *General Counsel*
DEBORAH G. BERNSTEIN, *Chief Clerk*
MARK H. GITENSTEIN, *Minority Chief Counsel*

SUBCOMMITTEE ON JUVENILE JUSTICE

ARLEN SPECTER, Pennsylvania, *Chairman*

JEREMIAH DENTON, Alabama
CHARLES McC. MATHIAS, JR., Maryland
MITCH McCONNELL, Kentucky

PAUL SIMON, Illinois
HOWARD M. METZENBAUM, Ohio

NEAL S. MANNE, *Counsel and Staff Director*
LAURIE WESTLEY, *Minority Chief Counsel*

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

CONTENTS

OPENING STATEMENTS

	Page
Trible, Hon. Paul S., Jr., a U.S. Senator from the State of Virginia	1
Denton, Hon. Jeremiah, a U.S. Senator from the State of Alabama	20
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania, chairman, Subcommittee on Juvenile Justice	23
McConnell, Hon. Mitch, a U.S. Senator from the State of Kentucky	27

PROPOSED LEGISLATION

S. 1305—Computer Pornography and Child Exploitation Prevention Act of 1985	4

CHRONOLOGICAL LIST OF WITNESSES

Lippe, Lawrence, Chief, General Litigation and Legal Advice Section, Criminal Division, U.S. Department of Justice	21
Smith, Hon. Jack D., General Counsel, Federal Communications Commission	28
Hudson, Hon. Henry, commonwealth's attorney, Arlington, VA; and Robert J. Humphreys, chief deputy commonwealth's attorney, Virginia Beach, VA	31
Taylor, Bruce A., general counsel, Citizens for Decency Through Law, Inc., Phoenix, AZ	37
Hartman, Paul M., U.S. Postal Inspection Service	46
Minot, George, Videotex Industry Association; and Thomas S. Warrick, Washington Apple Pi Computer Users' Association, accompanied by Joseph W. Chelena	50
Lynn, Barry W., legislative counsel, American Civil Liberties Union	73

ALPHABETICAL LISTING AND MATERIALS SUBMITTED

Denton, Hon. Jeremiah: Statement of Kenneth V. Lanning	9
Hartman, Paul M.: Testimony	46
Hudson, Hon. Henry: Testimony	31
Humphreys, Robert J.:	
Testimony	32
Prepared statement	35
Lippe, Lawrence: Testimony	21
Lynn, Barry W.: Testimony	73
Minot, George:	
Testimony	50
Text of bill drafted by VIA	53
Smith, Hon. Jack D.: Testimony	28
Taylor, Bruce A.:	
Testimony	37
Prepared statement	41
Warrick, Thomas S.:	
Testimony	59
Prepared statement of William J. Cook	61

APPENDIX

	Page
Statement of the American Sunbathing Association, Inc	81
Gallup poll—Most Americans Approve of Nude Recreation	88
Ohio Rev. Code	90
State of Ohio, plaintiff v. *George and Linda Robinson*, defendants	91
Letter to Senator Laxalt from Sheldon Elliot Steinbach, general counsel, American Council on Education	96
Statement of Walter R. Kurth, president of Associated Credit Bureaus, Inc	98

COMPUTER PORNOGRAPHY AND CHILD EXPLOITATION PREVENTION ACT

TUESDAY, OCTOBER 1, 1985

U.S. SENATE,
SUBCOMMITTEE ON JUVENILE JUSTICE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 385, Russell Senate Office Building, Hon. Arlen Specter (chairman of the subcommittee) presiding.

Also present: Senators Denton, McConnell, and Trible.

Staff present: Richard D. Holcomb (Senator Denton); Vic Maddox (Senator McConnell); Tracy McGee and Neal Manne (Subcommittee on Juvenile Justice); and Darren Trigonoplos (Senator Trible).

Senator DENTON. Good morning, ladies and gentlemen. Welcome to this hearing on S. 1305, the Computer Pornography and Child Exploitation Prevention Act of 1985.

Senator Specter, the subcommittee chairman, is testifying and has requested that I open the hearing in accordance with previous arrangements, turn the chair over to the sponsor of the bill, my friend and colleague from Virginia, Senator Trible.

OPENING STATEMENT OF HON. PAUL S. TRIBLE, JR., A U.S. SENATOR FROM THE STATE OF VIRGINIA

Senator TRIBLE. Thank you, Mr. Chairman.

The subcommittee is meeting today to receive testimony on the Computer Pornography and Child Exploitation Prevention Act, a bill I have sponsored together with Senator Denton and 12 other Senators. Senator Specter, the distinguished chairman of the Juvenile Justice Subcommittee, has asked that I chair today's hearing, and I am happy to oblige.

Today's hearing will address the use of computers and other means of interstate communications to facilitate crimes of child sexual abuse and child pornography, and to transport obscene matter.

Today's witnesses include Lawrence Lippe, Chief of the General Litigation Section of the Criminal Division, U.S. Justice Department; the Honorable Jack D. Smith, General Counsel to the Federal Communications Commission; the Honorable Henry Hudson, Commonwealth's attorney from Arlington, VA, and Chairman of the Attorney General's Commission on Pornography; Mr. Robert J. Humphreys, chief deputy Commonwealth's attorney from Virginia Beach, VA; Mr. Paul Hartman, an inspector with the U.S. Postal

Service; Mr. Bruce A. Taylor, an attorney with Citizens for Decency Through Law; Mr. George Minot, the chairman of the Executive Affairs Council, Videotex Industries Association; Mr. Thomas Warrick, president of the Washington Apple Pi Computer Users Association; and Mr. Barry W. Lynn, legislative counsel to the American Civil Liberties Union. The subcommittee will also receive written testimony from Mr. Paul J. McGeady, general counsel to Morality in Media, Inc.

The principal issue before us is the use of interstate means of communications to facilitate crimes of child molestation and child pornography. This would include both the Nation's mails and interstate computer transmissions.

At an oversight hearing on this subject in June, the Senate Subcommittee on Security and Terrorism heard that computers are becoming a favorite tool of child molesters, or pedophiles, for purposes of locating one another and exchanging information about their victims. The relative anonymity that computer communications provide appears to meet the pedophile's need to validate his behavior and share it with others.

For this reason, we will focus primarily on interstate communications by computer that facilitate acts of child sexual abuse.

Today's hearing will also address the use of interstate communications facilities, including computers, to facilitate the distribution of child pornography.

Finally, we will look closely at whether the existing prohibition in 18 U.S.C. 1462 on interstate transportation of obscenity applies to computer-transmitted material.

These are the general problems toward which S. 1305 is aimed.

Specifically, this bill will amend 18 U.S.C. 1462 to prohibit the interstate transmission of obscenity via computer. It would also create penalties for owners and operators of computer systems who knowingly engage in that same activity.

The bill will also amend 18 U.S.C. 2251 to create a "facilition" offense for activities that encourage or promote crimes of child molestation or the production of child pornography. Interstate communications, by computer or other means, whose intent is to facilitate such a crime would be proscribed.

Finally, S. 1305 will amend 18 U.S.C. 2252 to create an offense for interstate communications, by computer or other means, of advertisements to buy, sell, or trade child pornography.

This bill is one of many under review by Congress which address particular aspects of the problems of obscenity and child pornography. Last year, the Congress took an important step in this regard by approving the Child Protection Act. This measure has helped to strengthen the Federal Government's enforcement hand in cases involving the sexual exploitation of minors.

In addition, the President last year created the Attorney General's Commission on Pornography to reexamine the pornography industry and its effects on life in this Nation. We will hear today from the Commission's Chairman, Henry Hudson, with respect to certain child abuse cases in Virginia.

I cannot overestimate the importance of this effort. The explosive growth of the pornography industry over the past decade should be

a source of concern to all Americans. What was once a back-alley business is now a multibillion dollar industry.

Moreover, the content of pornographic material has changed markedly. Where simple nudity was once the order of the day, today's pornography features children, bondage, bestiality, and violence.

These changes are deeply troublesome. They presage a new and, I believe, more threatening sex industry.

To the extent that interstate means of communications and commerce are being employed to further this activity, it becomes incumbent upon the Congress to act.

On behalf of my absent colleagues this morning, I would ask unanimous consent that the hearing record be kept open for 30 days so they will have the opportunity to submit their questions and receive answers in writing.

At this point as well, I would ask unanimous consent to include in the record a copy of S. 1305 and a copy of Kenneth Lanning's testimony at the June 11 hearing on this subject.

Mr. Lanning cannot be with us today, but his June 11 testimony was quite helpful. Without objection, it is so ordered.

[Text of S. 1305 and Kenneth Lanning's testimony follow:]

II

99TH CONGRESS
1ST SESSION

S. 1305

To amend title 18, United States Code, to establish criminal penalties for the transmission by computer of obscene matter, or by computer or other means, of matter pertaining to the sexual exploitation of children, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 17 (legislative day, JUNE 3), 1985

Mr. TRIBLE (for himself and Mr. DENTON) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, to establish criminal penalties for the transmission by computer of obscene matter, or by computer or other means, of matter pertaining to the sexual exploitation of children, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Computer Pornography and Child Exploitation Prevention Act of 1985".

SEC. 2. Section 1462 of title 18, United States Code, is amended by—

(1) inserting after subsection (c) the following:

"(d) any obscene, lewd, lascivious, or filthy writing, description, picture, or other matter entered, stored, or transmitted by or in a computer; or

"Whoever knowingly owns, offers, provides, or operates any computer program or service having reasonable cause to believe that the computer program or computer service is being used to transmit in interstate or foreign commerce any matter the carriage of which is herein made unlawful; or"; and

(2) inserting at the end thereof the following:

"For purposes of this section—

"(1) the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;

"(2) the term 'computer program' means an instruction or statement or a series of instructions or statements in a form acceptable to a computer which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

"(3) the term 'computer service' includes computer time, data processing, and storage functions; and

"(4) the term 'computer system' means a set of related connected or unconnected computers, computer equipment, devices, and software.".

SEC. 3. (a) Section 2251 of title 18, United States Code, is amended—

(1) in subsection (a) by striking out "subsection (c)" and inserting in lieu thereof "subsection (d)";

(2) in subsection (b) by striking out "subsection (c)" and inserting in lieu thereof "subsection (d)";

(3) by redesignating subsection (c) as subsection (d); and

(4) by inserting after subsection (b) the following new subsection:

"(c) Any person who knowingly enters into or transmits by means of computer, or makes, prints, publishes, or reproduces by other means, or knowingly causes or allows to be entered into or transmitted by means of computer, or made, printed, published, or reproduced by other means—

"(1) any notice, statement or advertisement; or

"(2) any minors' name, telephone number, place of residence, physical characteristics, or other descriptive or identifying information,

for purposes of facilitating, encouraging, offering, or soliciting sexually explicit conduct of or with any minor, or the visual depiction of such conduct, shall be punished as provided in

subsection (d) of this section, if such person knows or has reason to know that such notice, statement, advertisement, or descriptive or identifying information will be transported in interstate or foreign commerce or mailed, or if such information has actually been transported in interstate or foreign commerce or mailed.".

SEC. 4. Section 2252 of title 18, United States Code, is amended—

(1) in subsection (a) by striking out "subsection (b)" and inserting in lieu thereof "subsection (c)";

(2) by redesignating subsection (b) as subsection (c);

(3) by inserting after subsection (a) the following new subsection:

"(b) Any person who knowingly enters into or transmits by means of computer, or makes, prints, publishes, or reproduces by other means, or knowingly causes or allows to be entered into or transmitted by means of computer, or made, printed, published, or reproduced by other means any notice, statement, or advertisement to buy, sell, receive, exchange, or disseminate any visual depiction, if—

"(1) the producing of such visual depiction involves the use of a minor engaging in sexual explicit conduct; and

"(2) such visual depiction is of such conduct;

shall be punished as provided under subsection (c), of this section, if such person knows or has reason to know that such notice, statement, or advertisement will be transported in interstate or foreign commerce or mailed, or if such notice, statement, or advertisement has actually been transported in interstate or foreign commerce or mailed.".

SEC. 5. Section 2255 of title 18, United States Code, is amended by adding at the end thereof the following new paragraph:

"(5) 'computer' means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility directly related to or operating in conjunction with such device.".

○

OPENING STATEMENT

OF

SPECIAL AGENT KENNETH V. LANNING

BEHAVIORAL SCIENCE UNIT

TRAINING DIVISION

FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON SECURITY AND TERRORISM

JUDICIARY COMMITTEE

UNITED STATES SENATE

REGARDING

USE OF COMPUTERS BY PEDOPHILES

Mr. Chairman and members of the subcommittee:

I am Special Agent Kenneth V. Lanning, a member of the Behavioral Science Unit of the FBI's Training Division. I am here today at the Chairman's invitation to provide information concerning the use of computers by pedophiles.

Introduction

A pedophile is typically a male individual with a sexual preference for children. His sexual fantasies and erotic imagery focus on children. Law enforcement investigations have verified that pedophiles almost always are collectors of child pornography and/or child erotica. They typically collect books, magazines, articles, newspapers, photographs, negatives, slides, movies, letters, diaries, sexual aids, souvenirs, toys, games, lists, paintings, ledgers, photographic equipment, etc., all relating to children in either a sexual, scientific, or social way. Not all pedophiles collect all these items. Their collections vary in size and scope.

Collection

What the pedophile collects can be divided into two categories. Child pornography can be behaviorally (although not

necessarily legally) defined as the sexually explicit reproduction of a child's image, voice or handwriting. In essense, it is the permanent record of the sexual abuse of a child. The only way you can produce child pornography is to sexually molest a child. Child pornography exists only for the consumption of pedophiles. If there were no pedophiles, there would be no child pornography. It includes sexually explicit photographs, negatives, slides, magazines, movies, video tapes, audio tapes, and handwritten notes.

Child erotica on the other hand, is a broader and more encompassing term. It can be defined as any material, relating to children, which serves a sexual purpose for a given individual. It is in a sense a subjective term, as almost anything potentially could serve a sexual purpose. However, some of the more common types of a child erotica include drawings, fantasy writings, diaries, souvenirs, sexual aids, manuals, letters and non-sexually explicit photographs of children. Generally, possession and distribution of these items do not constitute a violation of the law by themselves. However, besides possible legality, there is another important distinction between child pornography and child erotica. Although both may be used in similar ways by the pedophile, child pornography has the added and more important dimension of its effect on the child portrayed. Discussions and research on pornography often focus on the effects on the viewer rather than on the effects of the child subject. The latter is particularly crucial in evaluating the harm of child pornography.

Children used in pornography are desensitized and conditioned to respond as sexual objects. They are frequently ashamed of and/or embarassed about their portrayal in such material. They must deal with the permanency, longevity and circulation of such a record of their sexual abuse. Some types of sexual activity can be repressed and hidden from public knowledge; child victims can fantasize that some day the activity will be over and they can make a fresh start. But there is no denying or hiding from a sexually explicit photograph or video tape. The child in a photograph or video tape is young forever, and therefore the material

can be used over and over for years. Some children have even committed crimes in attempts to retrieve or destroy the permanent records of their molestation.

Whatever the reasons that pedophiles collect child pornography and erotica, its existence is undeniable and widespread. During any intervention or investigation of child sexual abuse, the possible presence of such material must be explored. For law enforcement officers, the existence and discovery of a child erotica and child pornography collection can be of invaluable assistance to the investigation of any child sexual abuse case. Obviously, child pornography itself is usually evidence of criminal violations. However, the ledgers, diaries, letters, books and souvenirs that are often part of a child erotica collection can also be used as supportive evidence to prove intent and for lead information. Names, addresses, and pictures of additional victims; dates and descriptions of sexual activity; names, addresses, phone numbers, and admissions of accomplices and other pedophiles; as well as descriptions of sexual fantasies, background information, and admissions of the subject are frequently part of a child erotica collection. Child erotica must be viewed in the context in which it is found. Although many people might have some similar items in their home, it is only the pedophile who collects such material for sexual purposes as part of his seduction of children.

Motivation

It is difficult to know with certainty why pedophiles collect child pornography and erotica. There may be as many reasons as there are pedophiles. Collecting this material may help pedophiles satisfy, deal with, or reinforce compulsive, persistent sexual fantasies about children.

Collecting may also fulfill needs for validation. Many pedophiles collect academic and scientific books and articles on the nature of pedophilia in an effort to understand and justify their behavior. For example, one such book states that research shows that children often participate willingly in sexual behavior with adults. One pedophile arrested by the police had in his

possession an article stating that children's sexual rights and freedom allow them access to pornographic materials and choice of sexual partners, including adults. Child molestation and incest would be criminal acts only if unwilling children were involved, the article went on to say. For the same reasons, pedophiles also frequently collect and sometimes distribute articles and manuals written by pedophiles in which they attempt to justify and rationalize their behavior as unblameworthy. In this material, pedophiles often share techniques for finding and seducing children and avoiding or dealing with the criminal justice system.

Collecting child erotica and pornography also appears to meet needs for camaraderie and additional behavior validation. Pedophiles swap pornographic photographs the way boys swap baseball cards. As they try to improve and upgrade their collections, they get strong reinforcement from each other for their behavior. It reinforces the belief that because others are doing the same thing it is not wrong. The collecting and trading become a common bond. Only another pedophile will understand, validate, and reward the behavior.

The need for validation may also partially explain why some pedophiles compulsively and systematically save the collected material. It is almost as though each communication and photograph is evidence of the value and legitimacy of their behavior. For example, one pedophile sends another pedophile a letter, enclosing photographs and describing his sexual activities with children. At the letter's conclusion he tells his fellow pedophile to destroy the letter because it could be damaging evidence against him. Six months later police find the letter while serving a search warrant. Not only has the letter not been destroyed, it has been carefully filed as part of the second pedophile's organized collection.

Pedophiles frequently collect and maintain lists of names, addresses, and phone numbers of persons with similar sexual interests, screening the names carefully and developing the list over a long time. The typical pedophile constantly seeks to

expand his correspondence. Names are obtained from advertisements in "swinger" magazines, pornography magazines, and even from legitimate newspapers. Correspondence usually begins carefully to avoid communicating with police. In many cases, however, the need to validate behavior continually and to share experiences overcomes concerns for safety. If mistakes lead to identification and arrest, the pedophile network often quickly alerts its members.

Another important motivation for collecting child pornography and erotica appears to stem from the fact that no matter how attractive any one child sexual partner is, there can be no long-term sexual relationship. All child victims will grow up and become sexually unattractive to the pedophile. However, in a photograph, a 9-year-old boy stays young forever.

Therefore pedophiles frequently maintain photographs of their victims. Some photographs may be sexually explicit, with the child nude or in varying stages of undress; in others the child is fully clothed. Although photographs of fully clothed children may not legally be considered child pornography, to the pedophile they are not much different from the sexually explicit photographs.

When photos are seized in a police raid, the pedophile may argue that photographs of fully dressed children are not part of the collection. In fact, they are an important part of the collection. The pedophile often keeps such photographs in his wallet. Many pedophiles even keep two sets of photographs of their victims. One set contains sexually explicit photographs; the other contains non-explicit photographs. Although this distinction may be important for criminal prosecution, to the pedophile each set might be equally stimulating and arousing. These victim photographs are like souvenirs or trophies of sexual relationships.

Uses of Child Pornography and Erotica

Although reasons why pedophiles collect child pornography and erotica are conjecture, we can be more certain of how this material is used. Study and police investigation have identified certain uses of the material.

Child pornography and child erotica are used for the sexual arousal and gratification of pedophiles. They use child pornography the same way other people use adult pornography - to feed sexual fantasies. Some pedophiles only collect and fantasize about the material without enacting these fantasies. In most cases coming to the attention of law enforcement, however, the arousal and fantasy fueled by the pornography is only a prelude to actual sexual activity with children.

A second use for child pornography and erotica is to lower children's inhibitions. A child who is reluctant to engage in sexual activity with an adult or to pose for sexually explicit photos can sometimes be convinced by viewing other children having "fun" participating in the activity. Peer pressure has a tremendous effect on children: if other children are involved, maybe it is all right, the child thinks. In the pornography used to lower inhibitions, the child portrayed will appear to be having a good time.

Books on human sexuality, sex education, and sex manuals are also used to lower inhibitions. Children are impressed by books, and they often believe that if something is in a book it must be acceptable. The controversial sex education book Show Me has been used by many pedophiles for this purpose. Adult pornography is also used, particularly with adolescent boy victims, to arouse and to lower inhibitions.

A third major use of child pornography collections is blackmail. If a pedophile already has a relationship with a child, seducing the child into sexual activity is only part of the plan. The pedophile must also ensure that the child maintains the "secret" and tells no one else of the activity. Pedophiles use many techniques to do so; one of them is through photographs taken of the child. If the child threatens to tell his or her parents or the authorities, the existence of sexually explicit photographs can be an effective silencer. The pedophile threatens to show the pictures to parents, friends, or teachers if the child reveals their secret.

A fourth use of child pornography and erotica is as a medium of exchange. Some pedophiles exchange photographs of children for access to or phone numbers of other children. The quality and theme of the material determines its value as an exchange medium. One Willie Mays baseball card may be worth two or three lesser cards; the same principle applies to child pornography. Rather than paying cash for access to a child, the pedophile may exchange a small part (usually duplicates) of his collection.

A fifth use of the collected material is for profit. Some people involved in the sale and distribution of child pornography are not pedophiles; they are involved to make money. In contrast, most pedophiles seem to collect child erotica and pornography for reasons other than profit. Others combine their pedophilic interests with the need to make money. Often they begin with nonprofit trading, which they pursue until they accumulate certain amounts or types of photographs, which are then sold to commercial dealers for reproduction in commercial child pornography magazines. Some collectors even have their own photographic reproduction equipment. Thus the photograph of a child, taken without parental knowledge by a neighborhood pedophile in a small American community can wind up in a commercial child pornography magazine with worldwide distribution.

The pedophile's collection usually has several important characteristics. These are as follows:

1. Important - The pedophile is willing to spend considerable time and money on the collection.

2. Constant - No matter how much the pedophile has, he never has enough; no matter how much he has, he never throws anything away.

3. Organized - The pedophile usually maintains detailed, neat, orderly records.

4. Permanent - The pedophile will move, hide, or give his collection to another pedophile, but will almost never destroy it.

5. Concealed - Because of the hidden or illegal nature of the pedophile's activity, the collection will be concealed but not to the extent that the pedophile does not have access.

6. Shared - The pedophile usually has a desire or need to show and tell others about his collection.

Computers

When you understand the needs of the pedophile and the characteristics of his collection, you begin to realize that there is a modern invention which would be of invaluable assistance to him. That invention is a computer. It could be a large computer system at his place of business or a small computer at his home. It is simply a matter of modern technology catching up with long time personality traits. The computer helps fill their needs for organization, souvenir records and validation.

Law Enforcement investigation has determined that pedophiles use computers in four major ways:

1. Storage and retrieval of information - Many pedophiles seem to be compulsive record keepers. A computer makes it much easier to store and retrieve names and addresses of victims and other pedophiles. Innumerable characteristics of victims and sexual acts can be easily recorded and analyzed. An extensive pornography collection can be catalogued by subject matter. Even fantasy writings and other narrative descriptions can be stored and retrieved for future use.

2. Communication - Many pedophiles communicate with other pedophiles. Now, instead of putting a stamp on a letter or package, they can use their computers and some necessary peripheral equipment to exchange information. The amount and type of information which can be exchanged is limited only by the equipment available.

3. Electronic Bulletin Board - Pedophiles can use their computers to locate individuals with similar interests. Like advertisements in "swinger magazines" electronic bulletin boards are used to identify individuals of mutual interest concerning age, gender and sexual preference. This use of the computer is not limited to pedophiles (see attachment A). In the December, 1983, issue of the NAMBLA Bulletin, a member from Michigan proposed that NAMBLA establish its own electronic bulletin board (see attachment B). Private communications firms offer message center services that allow computer users to have their messages duplicated and routed to designated receivers on the network. The pedophile may use an electronic bulletin board to which he has authorized access or he may illegally enter a system. It must be noted that the electronic bulletin board concept is a common and valuable use of a home computer. The pedophile merely uses this concept for his own needs.

4. Business records - Pedophiles who have turned their sexual interest in children and/or child pornography into a profit making business use computers the same way any business uses them. Lists of customers, dollar amounts of transactions, descriptions of inventory, etc., can all be kept track of by computer.

Conclusions

Pedophiles, as well as others involved in sex crimes, can and do use computers. Law enforcement officers must be alert for this valuable source of evidence and intelligence. In one recent case, a teenage "hacker" helped police break a pedophile's computer codes and thereby gain access to his records. Police

must be alert to the fact that any pedophile with intelligence, economic means or employment access might be using a computer in any or all of the above described ways.

Case Example

In a small southern city, police identified a pedophile named Ralph, who was sexually involved with more than 50 young boys in the local area. Pursuant to a search warrant, the police seized the following items believed to be of evidentiary value: photographic equipment, polaroid cameras, film, a typewriter, an address book, a calendar book, ledgers, cancelled checks, biorhythm charts, a computer, and computer tapes.

Ralph was a meticulous recordkeeper. He had a notebook with the names, addresses, and telephone numbers of many of his victims. He had a calendar book showing dates and types of sexual activity. He had a diary containing photographs and narrative information about over 50 victims. He had a small memoranda book which contained a summary and analysis of his sexual activity with 31 victims over a certain period of time. In this book, he recorded information such as the youngest (5.26 years), the oldest (19.45 years), and the average (10.89 years) age of his victims, the average duration of sexual relations (2.2 years), the average number of sex acts per person (64.68), the number of various types of sexual acts performed, the number of sperm ejaculated by his victims per day, and biorhythm information for each of his victims.

For many of his "regular" boys, he maintained even more information. For each of these boys he had a chronological list of sexual acts, with each act assigned a consecutive number. This was then cross-referenced to his account ledger for each boy. The ledger was a running balance of the amount of money each boy had on account. Money would be added for doing work around the house, for sexual acts, and for picture-taking sessions. Money would be subtracted for clothing, cigarettes, games, cash, and other presents. He kept the cancelled checks showing the payments

to each victim. He also had his victims make handwritten notes stating how much they enjoyed the sexual activity. He had photographs of the boys, many of which he kept in a green metal box.

The key to Ralph's meticulous recordkeeping was his computer. The computer contained information about sexual activity with over 400 boys and a few girls. He cross-referenced all the information he maintained on his victims. It contained a sexual history of each of his victims. He used it to keep track of the biorhythm charts of his victims. He also used it as an index for his child pornography collection so that he could locate photographs on specific sexual acts. The computer was accessed by using the name and an assigned bank account identification number of each victim. The computer also had a self-destruct program which the subject did not have an opportunity to initiate prior to his arrest.

Ralph's victims were primarily neighborhood boys whom he had befriended. He paid many of these boys for doing odd jobs around the house. His sexual acts with them consisted primarily of oral sex with the occasional anal sex. The subject always referred to the sexual acts as "projects". He frequently used alcohol to lower their inhibitions. Once the sexual acts began with the boys, he constantly reminded them not to tell anyone because it was their secret. He would attempt to justify the sexual acts by reading to his victims passages from the Bible which he claimed stated that this type of sex was of benefit to all humans.

All of Ralph's victims who were interviewed by the police stated that Ralph was a very nice man who was individually concerned with each of them. He paid them for work, sexual acts, and for photography sessions. He always encouraged the boys to compete with each other in the "projects". There were rewards of extra points and money for completing a sexual act better or longer than previously or better and longer than another boy. He created an "88 Club", in which a boy could become a member only after completing four different acts. Progress in joining this club was maintained on a chart.

After arresting Ralph, the police learned that he was on five-year's probation for sexually molesting children in another city. Ralph had also been convicted and served time for sexually molesting children 20 years earlier in another state. Ralph lied about this conviction on several job applications. Less than one month before his most recent discovery and arrest, Ralph's psychiatrist wrote a letter to his probation officer stating that "there is no indication that there has been recurrence of symptoms. I feel, therefore, that his problem remains in remission."

Senator TRIBLE. Senator Denton, would you care to make a statement?

OPENING STATEMENT OF HON. JEREMIAH DENTON, A U.S. SENATOR FROM THE STATE OF ALABAMA

Senator DENTON. Yes, Mr. Chairman.

I would like to compliment you for your leadership in introducing S. 1305, which establishes criminal penalties for transmission by computer of obscene matter or matter that pertains to the sexual exploitation of children.

Mr. Chairman, as you know, the rapid evolution of Federal communication channels has increased the technical complexities of regulating interstate communication in certain problem areas. There is great concern that pedophiles exchange names, addresses, and telephone numbers of their child victims by computer telephone hookup. There is evidence that the exchange of information supports the pedophile in his continued pattern of sexually molesting children. Concern for the problem prompted me, as chairman of the Subcommittee on Security and Terrorism, to conduct a hearing on the subject of the use of computers to transmit material inciting crime, particularly crimes involving the sexual abuse or exploitation of children.

At the June 11 hearing, Kenneth V. Lanning, supervisory special agent for the FBI, testified about the compulsive need of pedophiles and like-minded criminals to chronicle their exploits. Additionally, Mr. Lanning testified about the tendency of pedophiles to communicate their exploits to each other in order to validate, justify, and rationalize their behavior. Finally, Mr. Lanning stated that the computer helps to fill the needs of pedophiles for organization and validation, and can be used to communicate with like-minded criminals, thereby promoting the possibility of additional child abuse or exploitation.

The Subcommittee on Security and Terrorism also heard from representatives from the Federal Communications Commission and the Department of Justice, who stated that current prohibitions apparently do not apply to transmissions by computers over telephone lines. The prohibitions are found in section 223 of the Com-

munications Act, and in the Federal Obscenity Statute [18 U.S.C. 1462].

Mr. Chairman, I believe that it is appropriate for Congress to consider legislation that seeks to deter the transmission of information which facilitates sexual crimes against children over interstate telephone lines. As drafted, S. 1305 will help eliminate the use of interstate telecommunications facilities for the transmission of material relating to the sexual exploitation of children.

The bill will: First, expand the application of 18 U.S.C. 1462, which prohibits the importation or interstate transportation of obscene matter, to include a prohibition against the importation or transportation of such matter by computer; and second, expand the application of 18 U.S.C. 2251 and 2252, which prohibit the sexual exploitation of children, to include a prohibition against the transmission, by computer or otherwise, of data to facilitate such exploitation.

Mr. Chairman, as the U.S. Supreme Court noted in the famous case of *New York* v. *Ferber*, "The prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance." It is with that objective in mind that I offer my strong and continuing support to the Computer Pornography and Child Exploitation Prevention Act.

Mr. Chairman, I commend your leadership, and I look forward to passing the bill expeditiously.

Thank you, Mr. Chairman.

Senator TRIBLE. Thank you, Senator.

The 13 Members of the Senate sponsoring this legislation represent diverse political philosophies, but they are united in their concern about obscenity and the increasing use of computers to advance obscenity and to undermine the integrity of our society in terms of child pornography and child molestation.

The first witness this morning is Lawrence Lippe. Mr. Lippe is the Chief of the General Litigation and Legal Advice Section, Criminal Division of the U.S Department of Justice.

Mr. Lippe, please come forward.

STATEMENT OF LAWRENCE LIPPE, CHIEF, GENERAL LITIGATION AND LEGAL ADVICE SECTION, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. LIPPE. Thank you, Mr. Chairman and members of the subcommittee.

I am Larry Lippe, Chief of the General Litigation and Legal Advice Section of the Criminal Division of the U.S. Department of Justice. I have with me today Mr. Don Nicholson, who is a senior staff attorney in our section who has been for many years dealing in this matter of obscenity and child pornography, and I would appreciate having him here with me in the event he can assist in responding to any questions, should that become necessary.

I am pleased to testify today in strong support of the concepts and objectives embodied in S. 1305, the Computer Pornography and Child Exploitation Act of 1985.

Child molestation is conduct of the most heinous nature. Child abuse is punishable under many State and local laws, and we have

no reason to believe State and local authorities are not aggressively enforcing these laws. Nevertheless, there is a very valid role for the Federal Government to play.

In 1977, the Department of Justice strongly endorsed legislation which first banned the production and dissemination of child pornography. In 1984, the Department worked closely with Congress to develop legislation to strengthen these statutes. The legislation was enacted in May 1984. Since that time there has been a quantum leap in Federal prosecutions. Indeed, since last May we have indicted nearly twice as many defendants for violations of these statutes as during the prior 6½ years, and our conviction record has been impressive.

It should be clear that the Department places a very high priority on child pornography prosecutions. The Department enthusiastically endorses legislation which can increase our effectiveness in this area. As I stated earlier, the Department endorses the concepts reflected in S. 1305, and we believe this bill, with minor changes, can be an effective piece of legislation.

This bill would amend 18 U.S.C. 1462 to add obscene, lewd, lascivious, or filthy matter entered, stored, or transmitted by or in a computer to those items whose importation or interstate or foreign transportation by common carrier is presently forbidden by that statute. It would also punish those who knowingly permit their computer services to be used for the transmission of material covered by the statute in interstate or foreign commerce. In addition, the bill defines computer, computer program, computer service, and computer system.

The bill would also amend 18 U.S.C. 2251 to prohibit entry into or transmission by computer, or making, printing, publication, or reproduction by other means, of a notice, statement or advertisement, or of identifying information about minors, for the purpose of facilitating, encouraging, offering, or soliciting sexually explicit conduct with a minor, or the visual depiction of such conduct, if the actor knows or has reason to know the notice or other information will be transported in interstate or foreign commerce or mailed, or if it is in fact so transported or mailed.

The bill would amend 18 U.S.C. 2252 to prohibit entry into or transmission by computer or making, printing, publication, or reproduction by other means of a notice, statement, or advertisement to buy, sell, receive, exchange, or disseminate visual depictions of a minor engaging in sexually explicit conduct if the production of the visual depiction involves the use of a minor engaging in such conduct, and if the actor knows or has reason to know the notice, statement, or advertisement will be transported in interstate or foreign commerce or mailed, or if it is in fact so transported or mailed.

Finally, the bill would amend 18 U.S.C. 2255 by adding a definition of computer.

The intent of this legislation appears to be the prohibition of the use of computers for the interstate or foreign dissemination of obscene material, child pornography and advertisements for the same, and information about minors which can be used for child abuse. I shall first address what I consider to be the legal param-

eters of Federal legislation in this area. I shall then make certain recommendations for the restructuring of these provisions.

OPENING STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA, CHAIRMAN, SUBCOMMITTEE ON JUVENILE JUSTICE

Senator SPECTER. I was here earlier at 10, but the other Senators had not arrived, and I had other commitments. I regret that I cannot stay longer. I am going to submit questions for the record. I am going to turn the chairmanship over to Senator Trible at this time, with my commendation to him for his initiatives in the field, and the bill that is pending.

You may continue.

Mr. LIPPE. As I stated earlier, the Department of Justice fully supports S. 1305 in concept, and we strongly endorse those provisions of the bill that would ban the interstate or foreign dissemination by computer of obscene material, child pornography, and advertisements to buy, sell or trade child pornography. Federal statutes pertaining to pornography provide a comprehensive prohibition against the importation, mailing and interstate transmission of obscene material and child pornography (18 U.S.C. sections 1461, 1462, 1465, and 2252). Section 1461 also prohibits the mailing of advertisements for obscene material. Federal law also prohibits the use of children for the production of child pornography—18 U.S.C. section 2251—so long as the requisite interstate nexus can be established. Another statute prohibits the use of the telephone to make obscene comments—47 U.S.C. 223. Although some of these statutes purport to regulate the transmission of "obscene, lewd, lascivious, indecent, and filthy" material, Federal courts have construed all these words as being synonymous with the legal term "obscene." *Hamling* v. *United States,* 418 U.S. 87 (1974); *Manual Enterprises, Inc.* v. *Day,* 370 U.S. 478 (1962). While it might be argued that some of these statutes cover the use of a computer, explicit legislation on the subject is clearly desirable.

Such legislation would, we believe, pose no constitutional problem. It is abundantly clear that neither obscene material nor child pornography is protected by the first amendment. *New York* v. *Ferber,* 458 U.S. 747 (1982); *Miller* v. *California,* 413 U.S. 15 (1973).

The extent to which legislation may go beyond this point, to ban matter which is communicative in nature and neither obscene material nor child pornography is somewhat more problematic. As a general rule, the first amendment prohibits the Government from interfering with communication of factual information, *Richmond Newspapers, Inc.* v. *Virginia,* 448 U.S. 555 (1980); *First National Bank of Boston* v. *Bellotti,* 435 U.S. 765 (1978), even where the material communicated is of a commercial nature, *Virginia State Board of Pharmacy* v. *Virginia Citizens Consumer Council, Inc.,* 425 U.S. 748 (1976). In our view, legislation which seeks to ban the transmission of descriptive information about juveniles and nothing more would raise serious constitutional problems. This legislation, of course, is more limited because it imposes the condition that such information be provided "for purposes of facilitating, encouraging, offering, or soliciting sexually explicit conduct of or with

any minor." The question is whether this qualification is sufficient to cure any constitutional infirmity.

It is clear that the first amendment does not protect speech which is used as an integral part of conduct which is in violation of a valid criminal statute. *Giboney* v. *Empire Storage & Ice Co.,* 336 U.S. 490 (1949); *United States* v. *Barnett,* 667 F.2d 835 (9th Cir. 1982); *United States* v. *Moss,* 604 F.2d 569 (8th Cir. 1979). However, the courts have made a distinction between speech which merely advocates in general terms violation of the law and speech which is intended to incite imminent lawless activity; the former is protected speech, the latter is not. *Brandenberg* v. *Ohio,* 395 U.S. 444 (1969); *United States* v. *Damon,* 676 F.2d 1060 (5th Cir. 1982). Thus, it seems clear that Congress could ban the interstate or foreign dissemination by computer of information deemed speech which is involved with specific criminal activity.

There are existing precedents for such a Federal law. For instance, 18 U.S.C. 875 makes criminal the interstate communication of a telephone threat, and 18 U.S.C. 1084 makes it a criminal offense to use a wire communication facility for the transmission in interstate or foreign commerce of wagering information. Sections 1951 and 1952 of title 18 make criminal the threat to use physical violence to obstruct interstate commerce, and traveling in interstate commerce in connection with or to facilitate an "unlawful activity," as defined in the statute. It should be emphasized that all of these statutes cover speech which either constitutes or is intimately connected with illegel activity. They do not ban the communication of mere information.

Child abuse is essentially a local crime covered by local statutes, but so also is the underlying criminal conduct which is the subject of these four statutes. It is the interstate commerce aspect that provides the basis for Federal jurisdiction in these statutes, and that same basis would be available here. It is as appropriate for the Federal Government to assert jurisdiction over acts of child molestation facilitated by interstate computer transmissions or computer transmissions utilizing an interstate common carrier as it is for the Federal Government to assert jurisdiction over the crimes which underlie the four existing statutes.

However, a reading of the four cited statutes reveals that they all define the underlying criminal activity in such a specific fashion that it is clear the underlying activity is unlawful. The operative language in S. 1305 is not as precise. The statute as drafted could prohibit the exchange of identifying information which is innocuous on its face and where no underlying criminal activity is in being, imminent, or even specifically contemplated or planned. Under these circumstances, we are concerned that the proposed provisions would run afoul of the first amendment.

It may be suggested that the qualifying language in the proposed amendment to 18 U.S.C. 2251 is just as specific as the present language in that statute, particularly in light of the fact that "sexually explicit conduct" as used in the amendment would be limited by the definition of that term in 18 U.S.C. 2255. However, the new material sought to be covered by the proposed amendment is of a very different nature from what is dealt with in the present statutes. Section 2251 presently deals only with the production of child por-

nography, which is conduct involving actual child abuse, to which the first amendment is inapplicable. Section 2252 prohibits the dissemination of child pornography, which likewise has no first amendment protection. The amendment would add names, telephone numbers and other information about minors to the statute. This material is mere information which on its face may be content neutral and protected by the first amendment unless it is an integral part of conduct which is in violation of a criminal statute. It is neither conduct (present 2251) nor material which is unprotected per se (present 2252). A statute, such as the proposed amendment, which would ban the transmission of mere information must be more narrowly drawn—see Richmond Newspapers, First National Bank and Virginia State Board, supra—than one which deals with patently illegal conduct in order to withstand constitutional scrutiny.

We suggest that the language "for purposes of facilitating, encouraging, offering, or soliciting sexually explicit conduct of or with a minor" be amended by deleting the word "encouraging" and by adding the words "which sexually explicit conduct is in violation of any State or Federal law." As amended, the provision will read "for the purposes of facilitating, offering, or soliciting sexually explicit conduct of or with a minor which sexually explicit conduct is in violation of any State or Federal law." Tying the conduct to violations of specific statutes will, in our opinion, provide the necessary specificity to enable the statute to survive constitutional challenge.

I would like to turn now to some suggestions for restructuring the provisions of this bill.

If amended by the addition of proposed subsection (d), 18 U.S.C. 1462 would cover a person who imports a computer containing a covered program or uses a common carrier to ship it in interstate or foreign commerce. We understand the principal intent of proposed subsection (d) is to punish those who transmit covered material in interstate commerce from one computer to another via telephone lines. While a computer hooked up to a telephone line may be using a common carrier, this is by no means clear. We believe the desired coverage can be more effectively achieved by adding the words "or computer" after the words "common carrier" in the first paragraph of section 1462. Amending the statute in this fashion will obviate any possible controversy over whether use of a computer in the contemplated manner involves use of a "common carrier."

Under the present scheme of the child pornography statutes, 18 U.S.C. 2251 covers conduct, actual child abuse, and 18 U.S.C. 2252 deals with the dissemination of material. The proposed changes in this bill all concern the dissemination of material and, therefore, in our judgment, properly belong only in section 2252. Further, if the language "any notice, statement, or advertisement . . . for purposes of facilitating, encouraging, offering, or soliciting . . . the visual depiction of such conduct" in the proposed amendment to section 2251 means advertisements to buy or sell child pornography, it is duplicated by the proposed amendment to section 2252. If this language instead means a communication encouraging the production of such visual depictions, it is unnecessary because produc-

tion would require sexually explicit conduct by a minor, and communications encouraging such conduct are covered by other language of the proposed amendment to 18 U.S.C. 2251. We suggest that coverage of computer transmission of child pornography and advertisements to buy, sell, or trade it could be accomplished first, by amending 18 U.S.C. 2252(a)(1) to read "knowingly transports or ships in interstate or foreign commerce by any means, including by computer, or mails any visual depiction or any notice, statement, or advertisement to buy, sell, receive, exchange, or disseminate any visual depiction, if——;" second, by adding the words "by any means, including by computer," after the words "foreign commerce" where they appear in 18 U.S.C. 2252(a)(2); and third, by adding the words "or any notice, statement, or advertisement to buy, sell, receive, exchange, or disseminate any visual depiction" after the words "visual depiction" in the first two places in which they appear in 18 U.S.C. 2252(a)(2). A provision prohibiting the interstate or foreign dissemination of identifying information about minors, if amended as suggested above, could be added as a separate subsection of section 2252.

Finally, it has come to our attention that certain large providers of long-distance telephone service, such as AT&T and Sprint, either have or are attaining the capability of providing specialized computer services linked by telephone lines tailored to customer needs. To the extent that these companies provide such services as common carriers with neither control over nor knowledge of the content of these specialized networks, they should be exempt from liability. Since the amendments to all three statutes contain knowledge requirements, we view the bill as adequate to protect these service providers. However, we would suggest that the legislative history state that the legislation does not apply to providers of such services absent knowledge on their part or on the part of responsible corporate officers of the illegality of the transmissions.

I appreciate the opportunity to appear before you today to discuss S. 1305 and the issues involving the use of computers to transmit obscene material, child pornography, and information which is related to child abuse. The Department will be pleased to work with the staff of the subcommittee to draft appropriate language reflecting the Department's suggestions.

Thank you.

Senator TRIBLE. Mr. Lippe, I appreciate your strong support of this initiative. It is obviously our job to make this legislation as precise and as specific as possible, and we want to allay any concerns that have arisen. To that end, I think your contribution today is most helpful.

Senator McConnell has joined us, and I would like to turn to my distinguished colleague for an opening statement or questions.

Senator MCCONNELL. I want to thank my good friend from Virginia for bringing forth this legislation and ask that my opening statement appear in the record at this point.

[Statement follows:]

PREPARED STATEMENT OF HON. MITCH MCCONNELL, A U.S. SENATOR FROM THE STATE OF KENTUCKY

Mr. Chairman, I commend you for holding this hearing on this important bill, and for once again demonstrating the leadership you have consistently brought to the field of juvenile justice. I believe that Senator Trible's bill, S. 1305, raises some very important questions, and I am glad for the opportunity to study them in depth.

As you know, Mr. Chairman, one of the fundamental causes of child abuse and especially of child sexual exploitation is pedophilia. I learned while still chairman of the Kentucky Task Force on Exploited and Missing Children that thousands of children and adolescents are victimized by pedophiles each year. These children are sold by their own parents, or are forced into the seamy world of child pornography by hustlers, pimps and "benefactors." We don't know the extent of the problem, but we have no doubt about its seriousness. Any child or adolescent who is used in the child porn business, or who is patronized, which is to say, victimized by the pedophiles of this world is in serious danger.

Unfortunately, pedophiles are not unsophisticated, and they have now begun to use new and more clandestine ways of exchanging information, of cataloguing their victims, and of finding new ones. Senator Trible has identified perhaps the most troublesome new method—the computer bulletin board. By using that method of transmission, pedophiles are able to disseminate the information so critical to their disgusting practices, without running the risk of detection that other, more public means entail. And at present, they apparently do so without running the risk of criminal prosecution.

This bill would evidently change all that, and to that extent it is unassailable. Yet I must confess that I am troubled by the deeper implications of this legislation. This country cherishes the freedoms on which it is based. One of the great strengths of the United States is that its citizens are free to exchange information without government censorship.

Yet this bill would in one sense set up de facto governmental review or censorship. It evidently extends to conduct that involves merely offering a computer storage or transmission service if the offeror has "reasonable cause to know" that the computer is being used to transmit ary pedophilic matter. While seemingly innocuous, that sort of prohibition would require the operator of a computer service to regulate the content of the transmissions, or face criminal consequences. The chilling effect of such a provision should be apparent.

So while I applaud the intent of this legislation, there are some important questions that need yet to be answered. I'm confident that this hearing will take us a long way toward answering those questions, and I look forward to the testimony of the witnesses.

Thank you, Mr. Chairman.

Senator MCCONNELL. The subject, I think, is right in line with a lot of the initiatives that have been taken in the last few years in the whole field of missing and exploited children, and I think that this begins to address a new technology which may have a bearing on an area of crime that I happen to think is among the most offensive imaginable.

With that general observation, Paul, I will turn it back to you, and you may continue with the witnesses.

Senator TRIBLE. Thank you. I appreciate all of your help and support, Senator McConnell, and we will be submitting some detailed questions pursuing the points you have raised, but I think we should move on to the next witness at this time, Mr. Lippe. We thank you very much for your support and for your assistance and that of your colleagues in the Justice Department.

Mr. LIPPE. Thank you very much.

Senator TRIBLE. Next is the Honorable Jack D. Smith, general counsel for the Federal Communications Commission. He, too, testified in the June hearing on this subject.

Mr. Smith, you are most welcome. Your testimony will be made a part of the record in full. You are invited to summarize that testimony or give your full statement.

STATEMENT OF HON. JACK D. SMITH, GENERAL COUNSEL, FEDERAL COMMUNICATIONS COMMISSION

Mr. SMITH. Thank you, Chairman Trible, Senator McConnell.

Mr. Chairman and members of the subcommittee, I am pleased to participate in today's hearing on S. 1305, the Computer Pornography and Child Exploitation Prevention Act of 1985. Prior to the introduction of this measure by Senators Trible and Denton, I had the privilege of testifying before the Subcommittee on Security and Terrorism on the subject of whether Federal laws currently prohibit the transmission of obscene or indecent matter over interstate telecommunications facilities by means of computer.

Specifically, that hearing focused on the use of electronic bulletin boards by pedophiles or child molesters to encourage or facilitate the sexual exploitation of children. Before I address the merits of S. 1305, however, I believe a brief discussion of general background information is warranted so that my remarks will be viewed in the proper context.

Several types of computer bulletin boards are available to persons who wish to exchange information among each other. First, there are commercial public information services like Compuserve and The Source, whose subscribers can post private or public messages for each other. See Computer's Gazette, volume 2, No. 11, issue 17, November 1984. Some of these services even have online citizens band communications modes where messages can be sent by the transmitting computer to all recipients then on line.

Second, there are private bulletin boards which can be set up by as few as two friends. The hardware needed to operate a private bulletin board consists of only a computer, a modem, one or more phone lines, and appropriate storage devices. These types of private bulletin boards are relatively inexpensive; an owner of a personal computer could procure bulletin board software and all the necessary hardware for as little as $350. Then, other persons with knowledge of the telephone number of the bulletin board could gain access to any information on it. From information gleaned from the last hearing on S. 1305, it seems to be this latter type of private bulletin board which pedophiles are generally using to transmit information among themselves.

It is not, unfortunately, clear that the nefarious activities of pedophiles are proscribed by existing Federal law, at least where no crime is solicited, since the matter being transmitted may not necessarily be obscene or indecent per se. Therefore, if this activity is to be outlawed, legislation such as S. 1305 will be necessary. We at the FCC are extremely concerned about the proliferation of activities which employ interstate telecommunications facilities to further criminal enterprise, particularly those involving the sexual exploitation of children—activities that the framers of the Commnications Act did not envision. To protect children from this sort of exploitation, we support, in principle, the legislative initiative represented by S. 1305. As we have previously made some technical concerns known to Senator Trible's staff, I will confine my remarks to a few points I consider to be important to the overall effectiveness of the legislation before you today.

As introduced, S. 1305 would amend section 1462 of title 18, which prohibits the interstate transportation of obscene or similar matter. The bill would establish criminal penalties for using electronic bulletin boards to transmit matter which could be used to facilitate the sexual exploitation of children or to assist in the interstate transportation of such information. Further S. 1305 would amend section 2251 of title 18, which prohibits the sexual exploitation of children, to ensure that the use of communications common carrier facilities to transmit data to facilitate such exploitation is prohibited. Even though section 1462, which currently restricts carriage of obscene or similar material in interstate commerce by express companies or other common carriers, may currently apply to telephone companies, we would urge you to clarify that this section applies to interstate communications by means of wire or radio.

In this same vein, we believe the legislative history of this amendment should specify that the newly added phrase, "or interstate communications by means of wire or radio," includes all means of interstate communication, whether or not such communications are licensed as common carrier services, and whether or not traditional telephone lines or new technologies, such as the new fiberoptic and laser light technologies, are used. This could be accomplished by inserting the following definition of a communications system into the bill itself or its legislative history: Any common carrier or private system that itself is interstate or interconnected with interstate or foreign communications facilities.

Next, I would like to point out that the extent to which a constitutional right of privacy may apply to the use of electronic bulletin boards is insettled. Under the current law, the courts might require that a warrant be issued before a law enforcement officer could use information transmitted via electronic mail or posted on a private electronic bulletin board as a basis for a conviction. It may therefore be advisable for the legislative history to make clear the extent to which common law privacy rights are applicable to electronic data transmissions. This is particularly sensitive in the context of the electronic portions of systems used for private electronic mail, where it might be argued that users have an expectation of privacy comparable to that existing with respect to the post office.

While amending sections 1462 and 2251 of title 18 in the manner proposed by S. 1305 will adequately address the problem we seek to remedy, it is our view that the subcommittee should also consider amending the Federal racketeering statutes. For example, section 1952 of title 18, which prohibits the use of any facility of interstate commerce to distribute the proceeds of unlawful activities, to commit a crime of violence in furtherance of certain unlawful activities, or to otherwise promote such unlawful activities, could be amended to include child molestation or sexual exploitation as an unlawful activity. Alternatively, section 1953, which prohibits the use of interstate commerce to send materials to be used for bookmaking, could be amended to forbid the use of telephone facilities to transmit material which would encourage or facilitate crimes by pedophiles.

56-908 O - 86 - 2

Because all of the sections we seek to amend are contained in title 18 and, as a consequence, are outside our traditional area of expertise, we will, of course, defer to the Justice Department on the question of whether our proposed amendments to the racketeering provisions of title 18 would have advantages over those sections that S. 1305 would amend. I mention these alternatives only to ensure that the subcommittee has a chance to consider all available options in developing legislation to outlaw the activities of pedophiles.

Thank you for this opportunity to present the views of the FCC on this important legislation. We believe S. 1305, with the amendments we have recommended, will provide law enforcement officials with useful tools to combat the use of interstate telecommunications facilities to further criminal activities which sexually exploit children. I will be happy to answer any questions the subcommittee may have concerning my testimony.

Senator TRIBLE. Thank you for your testimony, Mr. Smith, and your continuing assistance in this regard. Your suggestions will be quite helpful as we formulate the final product of this legislation.

Senator McConnell.

Senator MCCONNELL. I do not have any questions right now, Mr. Chairman.

Senator TRIBLE. Mr. Smith, we will also submit some detailed questions to you as well, produced as a result of this hearing, and the testimony we hear as we move forward in fashioning this legislation.

Thank you for being here this morning.

Mr. SMITH. Thank you.

Senator TRIBLE. Before we hear from those witnesses who have investigated and prosecuted those types of cases, I would like to review a videotape. This segment is from a public television program entitled "Child at Risk," which was produced by KHUT television in Houston, TX.

What we will see is an attempt by an investigative reporter to locate and communicate via computer with pedophiles. While the type of communication shown here would not be an offense under S. 1305, the tape does provide some insight into the types of people with whom we are dealing and the types of communication in which they are engaged.

During the course of the tape, we will hear references to and a conversation with a member of NAMBLA. To clarify, this is simply an acronym for an organization called the North American Man-Boy Love Association.

Let us now proceed.

[Videotape shown.]

Senator TRIBLE. Let us turn now to two prosecuting attorneys who have dealt with this problem firsthand, Mr. Robert J. Humphreys, chief deputy Commonwealth's attorney, Virginia Beach, VA, and the Honorable Henry Hudson, Commonwealth's attorney, Arlington, VA.

Gentlemen, you are both most welcome.

Mr. Hudson, why do you not begin and then we will turn to Mr. Humphreys.

STATEMENT OF PANEL CONSISTING OF HON. HENRY HUDSON, COMMONWEALTH'S ATTORNEY, ARLINGTON, VA; AND ROBERT J. HUMPHREYS, CHIEF DEPUTY COMMONWEALTH'S ATTORNEY, VIRGINIA BEACH, VA

Mr. HUDSON. Thank you, Mr. Chairman, Senator McConnell.

My interest in S. 1305 flows from two sources: Regionally as a local prosecutor and nationally as chairman of the Attorney General's Commission on Pornography. In both capacities I have encountered instances where high technology has been utilized to promote commercial child sex syndicates. Contemporary research in the area of pedophilia has almost uniformly revealed that such persons tend to document their experiences and exchange such information among people similarly afflicted. Employing legitimate surveillance techniques, the U.S. Postal Service has developed methods of detecting some correspondence between identified practicing pedophiles. From these sources, numerous successful investigations have been launched, including several in northern Virginia. Consequently, people of this persuasion must resort to other clandestine means to exchange information. This, in my view, has spawned the types of communication systems addressed in part by S. 1305. Because of the technological sophistication of these systems, their interdiction has posed a considerable challenge to law enforcement officials.

In the Washington metropolitan area alone we have identified five computer systems presently in operation which communicate information pertaining to children disposed to engage in sexual activities with adults. These systems vary in content and mode of access, but are uniformly homosexual in orientation. Some harbor exclusively information on children, others a variety of age groups. In some jurisdictions cases involving these systems are still under investigation. Consequently, I cannot furnish specific details, but typically these five systems contain the following types of information concerning potential child sex partners: A code name or number for the child; age and physical description; sexual preferences; description of sexual parts; intelligence level; amount of financial consideration expected; method of contact; anecdotal experiences.

One system in the Washington metropolitan area reportedly has the capability of transmitting a photographic image of the child in question. The five systems that I have mentioned contain between 150 and 300 entries each. Based on an analysis of data available from these systems, it would appear that about 500 children have been the victim of sexual exploitation in our area alone.

Obviously, access to these systems is very controlled. In some instances, persons must pay a subscription fee to learn the access code. An additional surcharge is frequently exacted for access to data concerning children with a penchant for the more deviant forms of paraphilia. Other systems are simply maintained as a courtesy to other pedophiles and the access code is gained through affiliation with members of that subgroup. Once a person learns the access code, they simply call a designated telephone number, telephonically connect into the system, and punch in the appropriate code.

The data compiled in these systems is harvested from several sources. However, each of these children are in these systems because of a homosexual experience with a pedophile. In other words, each entry is graphic evidence of the sexual exploitation of a child. Law enforcement officials also know that almost without exception, pedophiles photograph their subjects to preserve the experience. Most such photographs are sexually explicit in nature. These photographs are also typically exchanged or sold among pedophiles. Often these photographs end up in sexually oriented publications without the knowledge or consent of the victim child. It would, therefore, appear that a well-defined nexus may exist between child pornography and the sexual exploitation of children. The Attorney General's Commission on Pornography has heard considerable evidence supporting that relationship.

I might add that the Commission will hear more detailed evidence on the relationship between pornography and the sexual abuse of children at its public hearings in Miami, FL, in November. We also intend to explore in some depth the role computers and high technology may play in the production and distribution of child pornography at that hearing.

S. 1305, if properly enforced by Federal authorities, could contribute substantially to a reduction in the sexual exploitation of a highly vulnerable sector of our society. Each of the computer systems discovered in the Washington metropolitan area utilize an interstate common carrier; that is, the telephone, as its communication medium. Information concerning such children is routinely conveyed between Virginia, Maryland, and the District of Columbia. The technological complexity of these systems and their multijurisdictional nature clearly warrants both Federal interest and jurisdiction. None of the individual component jurisdictions have an adequate legal means of combating this sinister service.

On behalf of law enforcement officials of northern Virginia, I want to express my appreciation for the leadership this subcommittee has shown in protecting the lives of our young people.

I will be glad to answer any questions you have, Mr. Trible.

Senator TRIBLE. Thank you.

Mr. Humphreys.

STATEMENT OF ROBERT J. HUMPHREYS

Mr. HUMPHREYS. Thank you, Mr. Chairman.

At the risk of trying to avoid echoing too much of what Henry had to say, I would like to depart from my prepared statement and make a couple of additional points, if I may, and echo much of what Henry had to say.

In South Hampton Roads, here in the State of Virginia, we have only one bulletin board of the type that Henry just described operating. That is in the city of Portsmouth, although it does service the entire South Hampton Roads area.

My presence here, I think, is the result of two criminal cases that we have ongoing presently in the city of Virginia Beach, and at the risk of trying to bring you the viewpoint from the trenches, I might say that what these two cases have in common, although they are otherwise unreleated, is the fact that computers were used

in different fashions in both of them. And I think these cases are still illustrative of the manner in which computers are being used by child molesters, child pornographers.

In one case the individual was a systems analyst by profession and had a profitable hobby of distributing and selling, in some cases, and in other cases, simply trading videotapes and eight millimeter films picturing juveniles ranging in age from approximately 6 to 7, up to teenage, 15, 16, 17, 18 years of age. This individual was not using his computer equipment in the manner which has been described so far here today. He was using it much in the manner of an electronic filing cabinet.

There is no question he was involved in interstate commerce. The portions of the mailing lists we were able to reconstruct indicates ties to 33 other States and two foreign countries. And although we have the computer disk containing the complete mailing list, it was constructed using an encryption program requiring a code to access it. We have obviously not gotten this individual's cooperation. We have thus far, notwithstanding the help of two Federal law enforcement agencies, and of a computer hacker, we have not been able to crack the code and access the entire mailing list. So, I think that this indicates one manner in which that computer was used, a secure filing system, if I can put it that way.

The other case we have presently ongoing occurred about 60 days later, and it seemed at first to be a rather ordinary child molesting case. There did not seem to be anything unusual about it until the individual who had been arrested for molesting an 11-year-old girl on a playqround proceeded to tell the investigating officer about his hobby, which was computers. He had a Radio Shack computer and proceeded to describe himself as a subscriber to one of these information systems, in this case, CompuServe. He proceeded to exchange fantasies and later information, including children's names and addresses, using codes, and whatnot, with individuals around the country.

He was, in effect, proud of the fact that he was combining his hobby with his sexual proclivities. We are in the process now of trying to find out the names of the individuals that he has dealt with. Frankly, that is pretty difficult.

CompuServe, certainly, is a reputable company; it is a subsidiary of H&R Block, and Mr. Minot is a senior vice president with that company, but the information in CompuServe is voluminous. You can make travel arrangements, you can look up encyclopedia articles, and you can conduct what amounts to citizens' band or CB conversations around the country for groups of people, and they can be scrambled, much in the way that secure communications are scrambled in the Defense Department, using a five- or six- or eight-letter word, you can conduct secure conversations. You can also leave electronic mail if you know the other individual's identification number, and it is as secure as you can get.

All of this is presently outside the reach of both State and Federal law, and S. 1305, I think, addresses that. We are in a situation locally where the police department, our police department, at least, and we are the largest city in Virginia, does not have the expertise to even detect, much less effectively investigate the types of crimes that are being committed. I think, in a nutshell, the best

way I can put it is the bad guys have the technological edge at this point, and there is no signs that we are able to catch up.

S. 1305, I think, addresses the problem. There is no question that we are dealing with interstate commerce, and we are not at the point where we are without the help of the Federal Government.

Local law enforcement cannot cope any more. I will be glad to answer any questions.

[Statement follows:]

Prepared Statement of Robert J. Humphreys

The first and primary duty of government at any level is the protection of its citizens. This is a duty owed in particular to our young, those unable protect themselves.

The degree to which our children are being molested and sexually exploited is reaching catastrophic proportions.

Those of us in the law enforcement community are challenged more and more by criminals whose activities benefit from a technological edge. The tools of the white-collar criminal have been discovered by the drug trafficker and more recently by the child molester and pornographer.

In my own city of Virginia Beach, within a period of sixty days, our police department arrested two individuals for felonies involving the sexual abuse of children. In both of these cases, the use of a computer has figured prominently.

In one of these cases, an individual has been indicted for the production and distribution of obscene materials which depict children. In connection with these charges, officers of the Virginia Beach Police Department seized over $40,000.00 worth of video equipment and more than 300 videotapes, eight millimeter films and still photographs.

Although the bulk of these items depict sexual activity between adults and various animals, sadism, bondage and master-slave relationships, we have identified approximately thirty videotapes and several dozen still photographs and slides which depict sexual activity between adults of both sexes and juveniles between the ages of six and fifteen years.

Also seized were such miscellaneous items as penis-shaped baby pacifiers and children's coloring books depicting sex with adults.

This particular individual was a computer programmer and systems analyst by profession and maintained his mailing list of suppliers and associates on a computer disk which is encoded to require a password to prevent unauthorized access.

The net result has been that although we have been able to show that this individual has mailed items to or received items from thirty-three states and two foreign countries, and although we have possession of the all important mailing list, the best attempts of computer experts in two federal agencies and one so-called "hacker" to unlock that list have been defeated by our inability to crack the code.

In a second and unrelated case which occurred two months later, an individual was arrested for molesting an eleven year old girl. Although there was nothing particularly unusual about the facts of the case, the suspect startled the investigating officer when he volunteered that he was a computer buff who owned a home computer and was communicating with other pedophiles through a computerized information service known as COMPUSERVE.

At this point, I must digress and advise you that COMPUSERVE, a wholly-owned subsidiary of H & R BLOCK, is a reputable corporation providing information to, and communications between, subscribers via a telephone linkage between the subscriber's computer and the COMPUSERVE system located in Columbus, Ohio.

Our suspect told his arresting officer that he would pursue his hobby and sexual appetites by using his home computer and his subscription to COMPUSERVE to identify others with a similar sexual preference for children, through one of COMPUSERVE'S interactive discussion forums and then communicate directly with them through COMPUSERVE'S electronic mail capability. He would then exchange information on methods used to attract children, and if the correspondent resided in close geographical proximity, the names of willing children.

It is important to note that although the interactive discussion forums are not private and can be accessed by any subscriber, the exchange of electronic letters is private and inaccessible to all but the sender, receiver and COMPUSERVE itself.

In my judgment these two cases illustrate the need for the passage of S.1305. The technological revolution has made the child molester and child pornographer a problem of interstate proportions which the states and localities can no longer deal with alone.

Senator TRIBLE. Gentlemen, I welcome your real world perspective. Those of us in Washington sometimes forget about the problems and the concerns of our communities, and I think you who are involved in the trenches fighting to keep our communities safe have an important perspective, and I thank you for sharing it today.

Certainly, the kinds of activities that you have sketched are a sickness that plague our society, and Congress simply cannot stand by and permit our children to be victimized. New technologies have offered new opportunities to child molesters and child pornographers, and we have to recognize that new reality and deal with it. That calls for strong action in our communities. It calls for more response from our States, and where there is a Federal nexus, surely it calls for a restructuring of Federal rules and Federal laws, so we can act in concert, and hopefully respond as society must to these kinds of activities.

Our purpose, obviously, is to ensure that our response is precise and specific and targeted to criminal behavior, and as a result of the hearing today, I believe that we will be able to successfully meet that criteria. We will have a bill that passes constitutional muster, and a bill that will give Federal law enforcement agencies the tools to respond forcefully and effectively to this criminal activity.

I thank you for being here. I commend your action and applaud your success and tenacity.

Our next witness is Mr. Bruce Taylor, general counsel of Citizens for Decency Through Law. Mr. Taylor has prosecuted hundreds of cases around the country.

I welcome his presence and expertise.

STATEMENT OF BRUCE A. TAYLOR, GENERAL COUNSEL, CITIZENS FOR DECENCY THROUGH LAW, INC., PHOENIX, AZ

Mr. TAYLOR. Thank you for having me, and I did put a written statement into the record, but I would like to take just a few minutes to summarize my thoughts on the subject instead of reading this statement.

As you know, Senator, the attorneys who work for CDL, and myself included, have a lot of experience in obscenity cases. I have handled about 600 in the city of Cleveland, OH, and have done about 60 jury trials, handled about a hundred appellate cases, and argued in the U.S. Supreme Court and various Federal courts. We see the problem on a daily basis both in the practical terms of what happens in the pornography industries, how it is involved with organized crime, and how it has spilled over in the child pornography trade, as well as a major underground activity of what is sometimes referred to as a cottage industry of pedophiles. We refer to pedophiles as just plain child molesters.

The bill as written, Senator, would, in my judgment, be both constitutional and upheld by the courts without further additions. It would also cover most of, if not practically all, the actual situations we are now seeing computers being used in, either to molest children, to advertise with the use of children, or to trade or sell child pornography. Porno syndicates do not use computers to sell pornog-

raphy. Individuals do use them to offer to trade or sell information leading to children.

It would be useful to clarify definitions in the bill such as what does a "communications system" mean, to look to the future of all the different forms of technology by including any "interstate communications by means of wire or radio" under the definition of "common carrier," and defining a communication system as "any common carrier or private system that itself is interstate or interconnected with interstate or foreign communications facilities." Those are good definitions. The FCC's suggestions are good suggestions.

One aspect that I would ask to be examined, and I propose this to the Department of Justice lawyers, and I would ask of the Congress' lawyers, too, those of us in the State prosecution network have also thought of section 1462, dealing with common carriers, to include—if the Department wished it to, and the courts, we think, would accept—Federal jurisdiction over intrastate carriage by a common carrier, meaning when a pornographer put material on a commerical carrier truck in downtown Cleveland and shipped it within the State. We assume, and there is a lot of case law relevant, that the Federal Government would have jurisdiction to arrest the pornographers, even though the shipment did not leave Ohio. If the Justice Department interprets "interstate commerce," as requiring that the material crosses State lines on a common carrier, that would make it a problem adding the word "computer" to the term "common carrier." I am sure it is not the intent of Congress to make any computer a common carrier under all circumstances, but you do want to include interstate phone line use of computers.

I think it has to be cleared up; does common carrier usage include intrastate as well as interstate commerce, and, if so, then you will have to restructure how you add computer to that term. It is one of those things to look forward to in the legal arguments that you are going to get from the lawyers on both sides. I think that is a function that we have always assumed, that the Federal Government could prosecute, but since this would still be an open question, you may not want to inadvertently make a computer a common carrier for all purposes. A telephone is a common carrier, and the Court ruled that in 1959, so any time a computer is hooked up to a telephone line, even if it is going from one side of a city to another, that would be an act of interstate commerce that the Bureau would have jurisdiction over even without the computer signal crossing the State line. So any time a computer is hooked up to a modem, this bill would confer Federal jurisdiction, even though the messages did not cross a State line. If common carrier is viewed in the same way, you would not have to make a computer a common carrier.

The knowingly requirement that the Senator referred to in your opening statement will, I think, as the Justice Department said, protect the rights of innocent companies like the phone company or computer services, or billboard operators, and the rights of High Society magazine which offers a pornographic swinger service through their computer system. That was the one that was normally looked at as one of the favorite targets of child molesters, be-

cause it was set up specifically for people trading in sex. High Society is advertising it for adults, but there is no way they can control it.

The knowing requirement that has been in the Federal statutes has been interpreted in two ways. The first goes to knowingly doing the act, meaning that you intentionally sell an item. The Government has to prove that you knew that you were selling something.

The second part of the requirement is knowledge of what it was, meaning knowledge of the general contents or the character of the material.

So when the statute says someone knowingly uses a computer system or has a computer system that they own that is knowingly being used to violate this section, it would require knowledge by corporate owners or the individual defendant. He knew that the information was being transferred; he knew it was intended to abuse the minor, and if it was child pornography, he knew the information contained pictures of minors. The bill, therefore, contains both those areas of intent and scienter.

They cannot be prosecuted unless the Government can prove that they not only knew what the messages were about, but they knew their services were being used to facilitate the abuse of a minor. The specific intent requirement is also in that same vein. The "mere information" comment and caveat that has been put in here, is that the Federal Government cannot regulate the transfer of mere information such as names and phone numbers. This bill goes further, however, and says you cannot transmit information about a child by computer for the specific purpose of abusing the child. That is much more like the mere evidence rule that says officers can seize a man's clothing or personal effects, even though those are not illegal, if you can prove they are specific evidence of the crime. It is not illegal to take a woman from one State to another unless the Government can prove why you were doing it, that is, prostitution. So the specific intent requirement is going to except this type of information about children from those cases which say the Government cannot pry into private businesses.

The other thing that bolsters this bill that is that the U.S. Supreme Court has recognized, in many cases especially dealing with customs, postal, and common carrier cases, that even private use of those facilities of interstate commerce can lead to jurisdiction under the criminal laws, even though there is no commercial intent.

Pedophiles use it for their own purposes. Therefore, it is unlike the interstate transportation of obscene materials, under section 1465, where you bring it in your own car or privately owned truck from one State to another, it has to be for sale or distribution. If you put it on a common carrier, or in the mail, or import it into the country, even from a husband to a wife, it is illegal. Federal laws say the border is to be free of obscenity. There, the bill as written will cover most, if not all, of the present uses of electronic devices we call computers or other items used to trade child pornography.

I think the changes suggested by the FCC will become useful in the future and prevent the Congress from having to relook at the

new technologies, and I think some of the clarifications the Department of Justice offered are devices to solve some of the appellate problems in defending the bill. But there are cases concerning the use of common carriers, the phone lines, and the mails that are almost identical to the intents of this crime, so that there will be enough support in existing law to uphold this bill in any of its facets.

The only suggestion that I would make is that Congress make an amendment or a clarification, concerning use of mails under section 1461, like you are trying to do with the use of computers, to do the same things that S. 1305 is trying to reach. If you use a computer to trade information on a kid for the purpose of abusing the child or to trade child pornography, it is a crime under S. 1305, but if you use the mails, it should also be a crime, since most pedophile exchanges are still done through the mail. Many times the Federal Government has had trouble in the past connecting some of the intents, such as, what the man wanted to do with it, or when the inspecter never actually closed the deal with the pedophile to get the pictures or see the child, so if the use of the mail to facilitate child pornography or abuse is made illegal and can be proven, the Government could close down a lot of this.

Thank you.

[Prepared statement follows:]

Prepared Statement of Bruce A. Taylor

Mr. Chairman and Members of the Subcommittee,

On behalf of CDL and myself, I thank you for inviting our comments on Senate Bill 1305. Citizens for Decency through Law, known as CDL, has been providing technical legal assistance to governmental, legislative, law enforcement, and citizens groups since 1957 and offers our knowledge and experience in obscenity cases and related First Amendment areas. Our staff is made up of former prosecutors with first hand dealings in how the pornography syndicates, organized crime, local distributors, and independent figures operate in distributing all forms of pornography and obscenity. This has necessarily led us to be involved with the newest and most serious development since hard-core pornography began to flourish in the early 1970's, and that is the progression and explosion of child pornography and the seductive or forcible rape of children. Whether a young boy or girl is a working prostitute, or whether they are seduced, coerced, or abducted by a molester is no real distinction. It is still rape, still criminal, and will always be the subject of government's strickest attention. The Supreme Court indicated the great extent that government can go to help solve this problem when it carved out a special exception to obscenity law in New York v. Ferber, 458 U.S. 747 (1982). The Court recognized that protecting children is a "compelling governmental" which justifies strong and novel measures to combat those who prey on young boys and girls. Detective Bill Dworin of the Los Angeles Police Department's Sexually Exploited Child Unit stated earlier this year that "There is so much child pornography here, that we can't even control that, much less other forms of pornography." Lt. Tom Rodgers of the Indianapolis Police Department has added that police can investigate child porn and abuse cases effectively, but they need new tools as the technology and sophistication of the offenders progress. These are two of the best experts in this field of crime, and they are telling us that the problem is real and very serious and that they are willing to work hard on it but they need government's help to be really effective. In our opinion, Senate Bill 1305 will help and we also believe it will be upheld in the courts.

S. 1305 is not a difficult law to analyze. Its provisions for knowingly using a common carrier and a computer to facilitate the illegal distribution of child pornography or using computers to facilitate the actual production of child porn or actual sexual abuse of children are well within established criminal law principles and legislative powers.

Use of Computers to Transmit Obscene Computer Pornography

Section 2 of the Bill would amend 18 U.S.C. § 1462 to cover the transmission of obscene depictions or descriptions by Computer over a common carrier, such as telephone lines. The Supreme Court has always held that obscene material is not protected by the First Amendment. Paris Adult Theatre v. Slation, 413 U.S. 49 (1973). The Court provided a definition of obscene in Miller v. California, 413 U.S. 15 (1973) and said that material is obscene if it meets the three part test and also gave "a few plain examples" of what kind of conduct could be regulated under that test if the material "depicts or describes" that conduct:

> (a) Patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated.
>
> (b) Patently offensive representations or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.

It is well established that obscenity can be depictions, representations, or descriptions, and can be made up entirely of words without pictures. Kaplan v. California, 413 U.S. 115 (1973). There is no need to spell out th "Miller Test" in federal statutes since the Supreme Court has construed the federal obscenity statutes, including Section 1462, to include the Miller guidelines within the terms "obscene, lewd, lascivious, or filthy". United States v. Orito, 413 U.S. 139 (1973); United States v. 12 200-Ft. Reels, 413 U.S. 123, 130 (1973); Hamling v. United States, 418 U.S. 87, 114 (1974). In U.S. v. Orito, at 143-44, the Court held that Congress has the power to prohibit interstate carriage under Section 1462 of obscene material, even for private use.

> Given (a) that obscene material is not protected under the First Amendment, Miller v. California, supra, Roth v. United States, supra, (b) that the Government has a legitimate interest in protecting the public commercial environment by preventing such material from entering the stream of commerce, see Paris Adult Theatre I, 413 U.S., at 45-64, 37 L.Ed.2d at 446, and (c) that no constitutionally protected privacy is involved, United States v. Thirty-Seven Photographs, supra, at 376, 28 L.Ed.2d 822

> (opinion of White, J.), we cannot say that the Constitution forbids comprehensive federal regulation of interstate transportation of obscene material merely because such transport may be private carriage, or because the material is intended for the private use of the transporter. That the transporter has an abstract proprietary power to shield the obscene material from all others and to guard the material with the same privacy as in the home is not controlling. Congress may regulate on the basis of the natural tendency of material in the home being kept private and the contrary tendency once material leaves that area, regardless of a transporter's professed intent. Congress could reasonable determine such regulation to be necessary to effect permissible federal control of interstate commerce in obscene material, based as that regulation is on a legislatively determined risk of ultimate exposure to juveniles or to the public and the harm that exposure could cause. See Paris adult Theatre I v. Slaton, . . .

The Court continued by noting that Congress could prohibit interstate transmission of lottery tickets, enticing women into other states for White Slave Traffic, and importation of pictorial representations of prize fights under its broad control over interstate commerce and the facilities of interstate commerce and communication. The Court concluded, at 144:

> "It is sufficient to reiterate the well-settled principle that Congress may impose relevant conditions and requirements on those who use the channels of interstate commerce inorder that those channels will not become the means of promoting or spreading evil, whether of a physical, moral or economic nature."

It is clear that this amendment would lawfully restrict only obscene, and therefore illegal, transmissions and will be upheld. The scienter requirement that the conduct be done "knowingly" will prevent abuse or restrictions on First Amendment and privacy rights. The Court has construed the word "knowingly" in federal statutes to mean a "knowledge of" or "reason to know" of the character or content of the depiction or description. Hamling, at 119-24. The Court pointed out that, "It is not innocent but calculated purveyance of filth which is exorcised. . . ."

This amendment has all the requirements needed to pass constitutional muster in the United States Supreme Court and will undoubtedly be upheld if passed.

Use of Computers to Facilitate Child Sexual Abuse or Exploitation

Section 3 of the Bill would amend Section 2251 to prohibit use of computers to transmit information about minors for purposes of facilitating the illegal sexual abuse or visual depiction of sexual abuse. This section would not prohibit innocent information about minors but only that which can be proven by the government to have illegal purposes. It is much like

the intent required by the White Slave Act upheld by the Court in Caminetti v. United States, 242 U.S. 470 (1917), and referred to in footnote 6 of U.S. v. Orito in 1973. Since the acts sought to be accomplished by a "knowing" offender are illegal acts, Congress may prohibit interstate commerce facilities, such as computers, from being used to facilitate such crimes. As noted in U.S. v. Orito, at 144, n.6, Congreess can regulate even when the ultimate act may not be a crime in the states or under federal law:

> 6. "Congress can certainly regulate interstate commerce to the extent of forbidding and punishing the use of such commerce as an agency to promote immorality, dishonesty of the spread of any evil or harm to the people of other States from the State of origin. In doing this it is merely excercising the police power, for the benefit of the public, within the field of interstate commerce. . . ."

This is true even in the First Amendment area, such as when the Court upheld the right of the federal government to prosecute the use of the mails to ship obscenity in Iowa even though the shipment was wholly intrastate and even though Iowa did not have a state statute making such obscenity illegal. Smith v. United States, 431 U.S. 291, 305 (1977). Both the scienter requirement and the specific intent requirement will satisfy constitutional requirements and the courts will uphold this section if passed.

Use of Computers to Disseminate Child Pornography

Section 4 of the Bill would amend Section 2252 to prohibit use of computers to facilitate the illegal dissemiantion of child pornography. Since the Court has held in Ferber that visual depictions of sexual abuse of minors is per se illegal, Congress can treat it as contraband and prohibit its transportation in interstate commerce or on facilities of such commerce. given the broad power recognized by the Supreme Court in the cases already discussed, it is not to be seriously doubted that the Court would deny the right to control modern technological means of violating an admittedly valid law. In United States v. Alpers, 338 U.S. 680 (1950), the Court held that phonograph records could be considered "matter" under Section 1426, even though they were a different medium from books and papers. The Court recognized that it was the illegal communication which

Congress can prohibit and changes in form and technology are not sufficient to defeat the reach of that power.

SUMMARY

As a practical matter, the government must prove under each of these three amendments that the offender used a computer in such a way, and with such knowledge and intent, to violate the statute as well as to come within federal jurisdiction over "interstate commerce". When using phone lines, the jurisdiction is clear, since telephone and telegraphy companies are common carriers. United States v. Radio Corp., 358 U.S. 334, 349 (1959). It has also been held that the physical objects themselves need not pass through interstate commerce or over the wires as long as the transfers of illegal information or funds is facilitated or accomplished by use of the wires. See: United States v. Gilboe, 684 F.2d 235, 238-39 (2d Cir. 1982). Congress has considerable power over these interstate communication systems, whether wire or broadcast. See F.C.C. v. Pacifica, 438 U.S. 726 (1978); No. Carolina Utilities Comm. v. F.C.C., 552 F.2d 1036 (4th Cir. 1977). It cannot be seriously doubted that these amendments will greatly aid law enforcement, will help protect children from unspeakable abuse, and will be found valid and constitutional. The only question remaining is how the Congress will vote. We hope and trust that Congress will vote positive and that this Bill becomes law at the earliest possible time. I have had considerable experience over the past 12 years in the field of obscenity prosecution. I've helped prosecute hundreds of cases, tried over sixty jury trials in several states, handled over two hundred appeals, and even argued before the Supreme Court. This experience has shown me the need for new laws as well as the gravity of the problem. CDL's involvement with federal and state law enforcement agencies will continue in the years to come, and we would welcome the tools to use which are set out in this Bill.

Respectfully submitted,

Citizens for Decency through Law, Inc.

By: Bruce A Taylor
Bruce A. Taylor
General Counsel

Senator TRIBLE. Thank you. As one who has prosecuted hundreds of criminal cases, I know how difficult it is to prove criminal intent. That is why the language reflects a necessity to prove an intent to violate the laws of the land.

Our objective is not to interfere with lawful activity. No innocent individual should be troubled by this legislation. The people who have reason to be concerned, however, are those who are engaged in child pornography, the sexual abuse of children, and those who transport obscene matter. That is our objective, and we are going to provide a vehicle for their successful prosecution.

Thank you, Mr. Taylor.

Next, we will hear from Mr. Paul M. Hartman of the U.S. Postal Inspection Service.

Mr. Hartman is an inspector with the U.S. Postal Service. He has investigated a number of computer transmissions among pedophiles. Mr. Hartman, once again, we welcome your real world experience. We thank you for underscoring the kinds of everyday problems entailed here.

STATEMENT OF PAUL M. HARTMAN, U.S. POSTAL INSPECTION SERVICE

Mr. HARTMAN. I am Postal Inspector Paul M. Hartman, an employee of the U.S. Postal Inspection Service. I am present today to offer testimony concerning the use of personal computers by pedophiles as a medium of communication

The U.S. Postal Inspection Service, among its many and varied responsibilities, is charged with the enforcement, in part, of the Child Protection Act of 1984, which was signed into law by President Reagan on May 21, 1984. Specifically, postal inspectors conduct investigations of the suspected use of the U.S. mails in the transmission and/or receipt of child pornographic materials. Such use of the mails is proscribed by 18 U.S.C. 2252.

My primary assignment is to conduct investigations into the use of the mails as a vehicle for traffic in child pornographic materials. Child pornography, which records the sexual molestation of children, is, by its very nature, the product and resource of pedophiles. Most of the investigations which I conduct are undercover in nature and cause me to come into frequent contact with pedophiles, persons who use children as sexual objects.

Due, perhaps, to the sanctions placed upon adult-child sexual relations within society, most pedophiles seek to conceal their sexual interest in children from family members, friends, and others with whom they come into regular social contact. As a result, they lack emotional and psychological support for their sexual interests and activities among their closest personal associates. Frequently, in order to satisfy the need to gain emotional and psychological acceptance and support, a pedophile will turn to another pedophile.

The use of the mails by pedophiles has long been recognized by postal inspectors as a mainstay of pedophiles' psychological support base. Letters provide a vehicle whereby individual pedophiles may share expressions of sympathy with one another, yet sufficiently protect the pedophiles' need for anonymity. As interpersonal relationships grow slowly through correspondence, confidence builds.

This confidence leads to an exchange of fantasies and accounts of actual sexual encounters with children. Further, this confidence often leads to an exchange of child pornographic materials, through the U.S. mails. Numerous investigations, conducted by me and other postal inspectors, have led to the recovery of this type of correspondence in the possession of offenders who were arrested for trafficking in child pornography.

When, during the course of an investigation, sufficient probable cause has been developed to indicate that a suspect has violated the child pornography statutes, a Federal search warrant is sought for the suspect's residence. Execution of search warrants usually leads to the recovery of child pornographic material and quantities of sexually oriented correspondence. It has not been uncommon for postal inspectors to seize personal computers and related materials that had been used to store data bearing on the identities of other pedophiles with whom the offenders have been in contact. Recently, however, I have learned through my own experience that pedophiles employ personal computers for purposes extending far beyond the mere storage of data.

I first became aware of the personal computer as a means of communication between pedophiles through correspondence with a person suspected of trafficking in child pornographic materials. The suspect described, in great detail, the advances in computer technology and the wonderful opportunities to meet new friends, other pedophiles. Shortly thereafter, I subscribed to the services of several firms, which, for a fee, provide access to computerized communication. With the use of a personal computer, already on hand in my office, I was soon communicating with pedophiles in various States throughout this country concerning child pornography and child involvement with sex.

In order for any person to communicate with another by way of computer, equipment requirements and skill levels are minimal. In addition to the personal computer, the only additional items necessary for computer communication are a modem, a rather inexpensive device, and access to a standard telephone line. The computer operator need have only a rudimentary knowledge of the equipment, provided by the owner's manual.

After having acquired the necessary equipment, the operator subscribes to the services of one of many firms which, for a fee, will grant the operator access to its computer. Further, the computer operator needs to acquire a working knowledge of the system commands, unique to each computer service. System commands are listed in literature provided by the firms, following subscription to the service.

There are currently a great many firms in the American marketplace offering access to computerized information and communication. These firms offer a wide variety of communications services, with varying degrees of security. The firms may offer subscribers access to electronic bulletin boards, which affords subscribers opportunities to publicly place and read messages. Such messages are accessible to all subscribers.

These firms may also offer subscribers a feature which permits one subscriber to send to another a confidential message, delivered by the computer only to the person for whom the message was in-

tended, much like the traditional letter. These messages are directed by the sender to the recipient by routing them to the recipient's identification number. Each subscriber is assigned a unique identifying number when subscribing to the service.

In a recent investigation, I accessed a computerized bulletin board and found a message, rather casually displayed, proclaiming another subscriber's interest in photographs of teen and preteen children. I formulated an electronic message and directed that message to the subscriber, who lives perhaps 2,000 miles away. Essentially, my message invited future contact. What followed was an exchange of electronic letters, via computer, in which the suspect offered to provide me with certain photographs. Ultimately, the suspect mailed to me photographs of a child, under the age of 18 years, which depicted that child engaged in sexually explicit conduct. That suspect has since been the subject of investigative attention by postal inspectors.

Notwithstanding the acknowledged existence of a number of activist pedophilic organizations many investigators, including I, have held to the belief that pedophiles, for the most part, are members of an underground subculture with no formal lines of communication of organizational structure. However, such is not the case with respect to a number of pedophiles who utilize computers to communicate about their sexual interests in and activities with children.

Many of the computer service firms offer additional features which pedophiles find attractive. One of these features provides subscribers the option to carry on private conversations, incapable of being monitored by other subscribers. The contemporaneous nature of this mode of communication, while satisfying the pedophiles' need for anonymity, facilitates the rapid development of interpersonal relationships between pedophiles. Those relationships are further strengthened when spontaneous dialog is offered through computers as compared to letters sent in the mail.

The conference feature, offered by many computer service firms, permits three or more subscribers to engage in contemporaneous dialog about matters of mutual interest. Conferences, however, can be monitored by any subscriber to the service and afford no measure of privacy to participants in the dialog.

Due to the sensitive nature of the information communicated between pedophiles, the need for privacy while in the conference mode is met by yet another feature offered by many of the computer service firms. Anonymity is maintained by the use of previously selected code words. In essence, subscribers privy to the code word enter it to communicate about child pornography so that other subscribers cannot monitor the conferences. The messages are encoded and decoded by the firm's computer, for only those subscribers who have input the agreed code word.

Acting in an undercover capacity, I have personally communicated with pedophiles, via a personal computer, in private and in conference communications. What I have learned through these various conversations has led me to believe that the instant communication capabilities available through a personal computer have afforded pedophiles opportunities to establish networks. These networks are comprised primarily of men bound by common interests,

pedophilia, and held together by a means of common communication, the personal computer. I have observed, within these networks, that one or two pedophiles will often assume leadership roles, coordinating the conversation and activities of other members of the network.

During computerized conversation with pedophiles, I have learned of pedophiles' actual and imagined sexual exploits with children; further, I have learned that pedophiles, who initially became acquainted through computerized communication, have escalated levels of contact to include telephone conversations and personal visits between one another. In certain instances, visits between pedophiles, who reside in different States, have been confirmed through independent investigation.

While engaged in computerized conversation with certain pedophiles, I have been introduced to yet other pedophiles, and have been referred to pedophiles who were alleged to be in a position to provide child pornographic materials. I have taken part in computerized conversations, during which pedophiles have identified, on a first name basis, children with whom they were currently sexually involved. In one such conversation, two pedophiles, although living hundreds of miles apart, spoke of common contacts with a child, now known to both.

Investigation into the activities of pedophiles who use personal computers has just begun. There is not currently available a fully developed body of information and experience to permit an assessment of the full impact of the role of the personal computer in the sexual exploitation of children. In the hands of the pedophile, I believe, the personal computer has become a useful tool for pedophiles to communicate with other pedophiles for the exploitation of children.

Senator TRIBLE. Mr. Hartman, I thank you for your testimony. You have described a host of criminal activities that are being advanced or implemented by use of the computer. Many of those activities are unlawful if the criminal actors use the mails, but are not unlawful today if they use computers, even though the mode of the transportation is still very similar. The reason for that, the authors of these laws did not envision new technologies, the computer traffic that moves across State lines. The most troubling aspect of your testimony to me is your view that there are actual networks in being, that a host of pedophiles around the country are in communication. They exchange the names of victims and, indeed, share the same victims, even though they live hundreds of miles apart.

The FBI, during the June 11 hearing, said that while they have no specific estimate of the numbers of pedophiles involved in this kind of networking, that they believe it is extensive, that they view it as a national problem, and indeed an international problem.

Would that assessment square with your own experience and your concerns of what the future holds for the use of computers and the networking that ensues?

Mr. HARTMAN. Yes, it would, Senator. What I found, after having entered this area of investigation, was a level of activity and openness that far exceeded what I had anticipated before entering it.

Senator TRIBLE. Mr. Hartman, I am glad you are here, and I thank you again for sharing your own experience. I think it underscores how pervasive this problem has already become, and I think it underscores the magnitude of the challenge.

Thank you very much.

Mr. HARTMAN. Thank you.

Senator TRIBLE. Next we will hear from two gentlemen, Mr. George Minot of the Videotex Industries Association, and Mr. Thomas S. Warrick, Washington Apple Pi Computer Users' Association.

STATEMENT OF PANEL CONSISTING OF GEORGE MINOT, VIDEOTEX INDUSTRY ASSOCIATION; AND THOMAS S. WARRICK, WASHINGTON APPLE PI COMPUTER USERS' ASSOCIATION, ACCOMPANIED BY JOSEPH W. CHELENA

Mr. MINOT. Thank you, Senator.

I am George Minot, senior vice president of CompuServe Inc. and chairman of the Videotex Industry Association's External Affairs Council. CompuServe is a $70 million remote computing services organization headquartered in Columbus, OH. We are one of the videotex pioneers and a leading provider of information services to industry, the business community, Government and consumers. The Videotex Industry Association is a trade group comprised of over 160 companies interested in furthering the development of videotex in North America. The External Affairs Council is the group within the VIA that has been given the responsibility to address issues relating to the misuse of computer resources, including but not limited to unauthorized attempts, unauthorized connections, theft-of-service, theft-of-property, destruction of property, and invasion of privacy.

To understand how the misuse of computers affects our rapidly emerging industry, it is important to understand the features and capabilities of videotex. Videotex is a relatively new communications technology which enables an individual with a personal computer, computer terminal or a videotex device connected to a television set, to access a variety of computer-based information databases, usually via telephone lines. Videotex also enables individuals to send/receive electronic messages and conduct financial transactions, such as transfers of funds, payments of bills and purchases of goods and services. Videotex is currently being developed for both home and business applications. CompuServe currently has more than 275,000 subscribers to its public videotex service and has contracted with more than 100 corporate clients to install in-house videotex systems using our host computers and databases. A leading research firm recently projected that by 1988 the number of people subscribing to videotex services will hit 4.2 million. Every major company in the United States will be using some form of videotex by the end of this century.

CompuServe, like many videotex systems operators, sponsors bulletin boards and forums allowing individuals with similar interests to communicate with each other in various ways. If subscribers register complaints with us concerning the content of certain databases or undesirable electronic messages directed to them, we in-

vestigate the complaints and attempt to convince the information provider or initiator of the objectionable message to discontinue the practice. If the situation persists, we take appropriate corrective action. Thus, I believe that CompuServe as well as other responsible videotex system operators are already taking significant steps to discourage computer misuse.

We in the videotex industry wholeheartedly support efforts to address the critical problems of child abuse and sexual exploitation of children. We support the goal of making it more difficult for child molesters and pornographers to exploit juveniles. We also support the prohibition of the use of various media by child molesters and pornographers transmitting obscene material so long as it does not affect individuals' first amendment rights. But we cannot support the language of this bill for two reasons. First, the bill, as written, is too narrowly focused—we feel these issues could be more appropriately addressed within the context of an omnibus computer crime bill. Second, we believe the bill will require vdeotex system operators to determine what materials/messages are or are not obscene—a task which we are not qualified in any way to carry out.

The transmission of obscene material is just one of many illegal activities that can take place using computer resources. Individuals often use bulletin boards to publish illegally obtained access codes and credit card numbers, to share techniques on breaking into computer systems–even to share recipes for making bombs, hand grenades, and molotov cocktails. There is no Federal statute covering any of these reprehensible activities, for the Federal computer crime bill passed last year applies only to the use of Government computer resources. What is really needed is an omnibus bill which specifically addresses all forms of computer abuse—from the transmission of obscene material to the publishing of secret access codes to unauthorized access to the distruction of computer databases. I suggest the computer crime bill that you are sponsoring, Senator Trible, S. 440, appears to me to be an excellent place to start building the omnibus legislation needed to address the wide variety of issues dealing with the public misuse of computers. I would also suggest you review the Model Computer Crime Act the VIA has drafted, which I believe addresses many of your concerns about the misuse of computers. A copy of this draft bill is attached to the testimony, and I would request it be included in the record.

Many State legislatures have now passed legislation concerning the misuse of computers. Most of those so-called computer crime bills are so narrowly focused as to be little help to prosecutors, who generally have little or no expertise in the computer crime arena. In order to be effective, prosecutors need broad language that defines a multitude of computer crimes which can be prosecuted under the law. If Congress uses this same piecemeal approach, attempting to modify existing laws or pass new bills to cover each different form of computer abuse, it will be almost impossible for our rapidly emerging industry to focus the public support we need to obtain effective law enforcement.

The other reason we do not sopport this legislation is that it may require videotex system operators to unilaterally determine whether or not material supplied by third parties is obscene. This bill indicates that any person who knowingly allows to be transmitted by

means of a computer, any pornographic or obscene material, shall be punished according to the provisions outlined. We believe any person could easily be interpreted as a videotex system operator. This would require system operators such as CompuServe to continuously preview all third-party databases and monitor all special interest group sessions, forums, bulletin boards and electronic mail messages—thus forcing us to perform a judicial role as well as invade the privacy of our own subscribers.

Even if we could monitor all the material on our systems—which I do not believe is practical—we as videotex system operators are not qualified to determine what is obscene and what is not. Individuals' definitions of pornographic and obscene material vary greatly. If one of our subscribers accesses a portion of our service that he or she deems objectionable, that subscriber is free to exit that portion and enter a different database. We do not believe system operators should be required to assume the role of judge and jury or invade the privacy of individuals.

As our society becomes more and more computer literate and more and more personal computers are installed in businesses and homes, the potential for widespread computer abuse of all kinds will grow exponentially. You, our chosen few, must ensure that laws are passed to adequately address not only the computer pornography and child exploitation problems but also the other crucial computer crime issues. We understand that S. 1305 is a living document, and that you are receptive to ideas on how to improve the bill's language. Mr. Chairman, I trust that our testimony here today has provided some useful ideas, and we at the VIA look forward to working closely with you in the near future to assist, in any way we can, in enacting comprehensive computer crime legislation that will help alleviate all of our concerns about the misuse of computers, computer systems, computer services and computer networks by all types of criminals.

Senator TRIBLE. Thank you, Mr. Minot.

[Text of bill drafted by VIA follows:]

A BILL

To amend title 18 of the United States Code to provide additional penalties for fraud and related activities in connection with computers and access devices, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE

SECTION 1. This act may be cited as the "National Computer Crime Act of 1985".

SECTION 1030 AMENDMENTS

SECTION 2. Section 1030 of Title 18 of the United States Code is amended -

(1) by striking out "or" at the end of paragraph (2) of subsection (a);

(2) by inserting after paragraph 3 of subsection (a), but before "shall be punished", the following new paragraphs:

"(4) having devised a scheme or artifice to defraud, knowingly and with intent to execute such scheme or artifice, accesses, permits access to, causes to be accessed or attempts to access a computer, computer network, computer software, computer data, computer program or computer supplies without authorization, or having obtained such access with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and obtains anything of value, and affects interstate or foreign commerce;

"(5) having intended to devise a scheme or artifice to defraud, knowingly and with intent to devise such a scheme or artifice to defraud, accesses, permits access to, causes to be accessed or attempts to access a computer, computer network, computer software, computer data, computer program or computer supplies without authorization, or having obtained such access with authorization, uses the opportunity such access provides for purposes to which such authorization does

not extend, and such scheme or artifice to defraud, if carried out, would affect interstate or foreign commerce;

"(6) knowingly damages, destroys or alters any part of a computer, computer network, computer data, computer software, computer program or computer supplies and affects interstate or foreign commerce;

"(7) knowingly and without authorization accesses, permits access to, or causes to be accessed, a computer, computer network, computer software, computer data, computer program or computer supplies which operates in or uses a facility of interstate or foreign commerce;

"(8) knowingly and without authorization takes, transfers, discloses, obtains, copies, uses or retains possession of all or any part of a computer, computer software, computer program, computer data, computer supplies or computer resources and affects interstate or foreign commerce;

"(9) knowingly and without authorization obtains and discloses, publishes, transfers, or uses an access device and affects interstate or foreign commerce;

"(10) knowingly interferes with or denies access to an authorized user or the use by an authorized user of a computer or computer network, which operates in, or uses a facility of interstate or foreign commerce; or

"(11) knowingly creates or causes to created computer data which purports to be genuine but which in fact is not because it has been falsely made, altered, deleted, added to or created by the combination of parts of two or more genuine pieces of computer data, and affects interstate or foreign commerce";

(3) by striking out the last sentence in subsection (a);

(4) by inserting after "(a)(1)" each place it appears in subsection (c)(1) the following: "(a)(4), (a)(5), (a)(6), (a)(9) or (a)(11)";

(5) by striking out "or (a)(3)" each place it appears in subsection (c)(2) and inserting in lieu thereof the following: "(a)(3), (a)(7), (a)(8) or (a)(10)";

(6) by inserting at the end of subsection (d) the following new sentence: "This subsection does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, nor does it prohibit prosecution pursuant to any other statute".

(7) by striking out subsection (e) and inserting the following new subsection:

"(e) As used in this section, the term 'computer' means an electronic, magnetic, optical, hydraulic or electrochemical device or group of devices which pursuant to computer program, to human instruction or to permanent instructions contained in a device or group of devices can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term computer includes any connected or directly related device, equipment or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device;"

(8) by adding at the end of such section the following new subsections:

"(f) As used in this section, the term 'access' means to intercept, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer network or computer data;

"(g) As used in this section, the term 'access device' means a card, code or other means of identification, or any combination thereof, that may be used for the purpose of accessing or using a computer,

computer network, computer program or computer software;

"(h) As used in this section, the term 'computer data' means any representation of knowledge, facts, concepts, instructions or other information computed, classified, processed, transmitted, received, retrieved, originated, switched, stored, manifested, measured, detected, recorded, reproduced, handled or utilized by a computer, computer network or computer software and may be in any medium, including but not limited to computer printouts, microfilm, microfiche, magnetic storage media, optical storage media, punched paper tape, or punchcards, or it may be stored internally in the memory of a computer;

"(i) As used in this section, the term 'computer network' means a set of related, remotely connected devices and any communications facilities including more than one computer with the capabiilty to transmit computer data among them through the communications facilities;

"(j) As used in this section, the term 'computer program' means an ordered set of data representing instructions or statements, in a form readable by a computer, which controls, directs or otherwise influences the functioning of a computer or computer network.

"(k) As used in this section, the term 'computer resources' includes, but is not limited to, information retrieval; data processing, transmission and storage; and other functions performed, in whole or in part, by the use of computers, computer networks or computer programs.

"(l) As used in this section, the term 'computer software' means a series of instructions or statements, which when put in a form readable by a computer functions as a computer program. 'Computer software' also means all procedures and associated documentation

concerned with the operation of a computer or a computer network.

"(m) As used in this section, the term 'computer supplies' means punchcards, paper tape, magnetic tape, disk packs, diskettes, paper, microfilm, and any other tangible input, output or storage medium used in connection with a computer, computer network, computer software, computer program or computer data.

"(n) As used in this section, the term 'person' shall include any individual, partnership, association, corporation or joint venture.

"(o) For purposes of subsection (a), an employee, unless it is established otherwise, shall be presumed to have authority to access and use any computer, computer network, computer software, computer program, computer resources or computer data owned or operated by the employer of such employee;

"(p) Injunctive relief - whenever it shall appear that any person is engaged or about to engage in any act which constitutes or will constitute a violation of this chapter, the Attorney General or any person injured or who would be injured by such violation may initiate a civil proceeding in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

"(q)(1) Civil actions - Any person whose property or person shall be injured by reason of a violation of any provision of this chapter may sue therefor and recover any damages sustained, and the costs of suit, including reasonable attorneys' fees, expert witness fees and costs of investigation. Without limiting the generality of the term, 'damages' shall include loss of profits and consequential damages;

"(2) At the request of any party to an action brought pursuant to subsection (q), the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect the trade secrets of any party;

"(3) The provisions of this chapter shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by any statute or common law;

"(4) A civil action under subsection (q) must be commenced before the earlier of (i) five years after the last act in the course of conduct constituting a violation of this chapter or (ii) two years after the plaintiff discovers or should have reasonably discovered the last act in the course of conduct constituting a violation of this chapter.

"(r) Venue - venue for any civil action brought pursuant to this chapter shall be in any county or city where the computer, computer network, computer software, computer program or computer data, which is accessed, is located in whole or in part at the time of the unlawful act, or in any county or city where the offender or owner resides or maintains a place of business."

Senator TRIBLE. Mr. Warrick.

STATEMENT OF THOMAS S. WARRICK

Mr. WARRICK. Mr. Chairman and members of the committee, my name is Thomas S. Warrick. I am an associate with the law firm of Pierson, Semmes & Finley here in Washington. Most of my professional time is spent representing American claimants against the Government of Iran before the Iran-United States Claims Tribunal in The Hague. My practice has also included litigation of constitutional issues and computer law. In my spare time, I am the president of Washington Apple Pi, Ltd. [WAP], a nonprofit association of Apple computer owners most of whom live in the greater Washington, DC area. For 3 years, before I was elected to my current position, I was our group's computer bulletin board system operator.

With me is Joseph W. Chelena, the economist who analyzes the microcomputer, television, and audio industries for the U.S. Department of Labor's Consumer Price Index. Mr. Chelena is currently one of our group's bulletin board system operators.

Mr. Chairman, we thank you for inviting us to assist the subcommittee in its consideration of S. 1305, a bill to amend the Federal Criminal Code to establish penalties for the transmission of obscene matter and matter pertaining to the sexual exploitation of children. As a nonprofit organization of microcomputer users, Washington Apple Pi does not take a position on legislation. We do have, though, the considerable expertise of our many members in how microcomputers operate and how they are used. We are most willing to make that expertise available to the subcommittee in any way we can.

Even though Washington Apple Pi does not formally take a position on S. 1305, Mr. Chairman, we are able to say that there is much in S. 1305 that we think everyone, not just our members, would support. Specifically, one, we support the principle that computer communications should be treated no differently than spoken, written, telephonic, print, or visual means of communication. They should have neither greater nor lesser status.

Two, we support the principle that competent adults who commit crimes should be held responsible for their criminal conduct.

Three, we support the prevention of sexual exploitation of children by adults.

Unfortunately, in accomplishing those worthwhile goals, S. 1305 in its present form would have certain unintended effects on computer bulletin board systems that would effectively destroy this new and promising means of communication. S. 1305 in its present form would also have a destructive effect on electronic mail services and online information suppliers upon which businesses and individuals have come to depend for transmission of important, time-sensitive information. The bill would also inhibit business and the Government from linking already-existing computers together in efficient, cost-effective ways. Washington Apple Pi is interested in assisting in any way it can so that these inadvertent side effects do not detract from the three important objectives we see in S. 1305 that we outlined above.

What is Washington Apple Pi? Washington Apple Pi is an organization of 5,000 members, most of whom live in Virginia, Maryland and the District of Columbia. We also have members in virtually every State and around the world. Our members range from people who are computer illiterates and proud of it, to some of the finest minds in the computer industry. Our members include young students and leaders of Fortune 100 companies, members of religious orders and even some people on Capitol Hill.

Washington Apple Pi serves as a center of learning for everyone interested in personal computers, particularly Apple and Macintosh computers. We are a not-for-profit organization of volunteers who keep ourselves up to date on the growing computer technology and who provide information that makes personal computers more understandable and usable in everyday life, whether for business, education, science, self-expression, or fun.

WAP maintains a small office in the suburbs with volunteers and a few paid staff. We publish a monthly journal, free to all members. One of our most important services is a hot line of volunteers who are able to help people with questions and problems using their computers. We have one of the finest collections of microcomputer books and magazines to be found outside of Congress' own library. We make available to our members thousands of public-domain computer programs of all kinds. In addition, WAP has a number of special interest groups on topics such as education, computer applications for the disabled, investors, and specialized computer programming languages.

Among Washington Apple Pi's most popular services for members are our computer bulletin board systems. WAP presently runs four in the area, some out of our office and some out of spare rooms in the homes of several of our members. These systems each average 50 to 60 calls a day, and the demand is such that we are adding more systems when we can.

Unable to be here is Mr. William J. Cook, a journalist for Newsweek magazine, who is also the author of "The Joy of Computer Communication." He is one of the best people available to advise the committee in understanding how personal computers can be used. I would also ask that his testimony be made a part of the record.

Senator TRIBLE. Mr. Cook is most welcome. His testimony will be made a part of the record.

[Statement follows:]

Testimony of

William J. Cook

Mr. Chairman and members of the committee, my name is William J. Cook. I am a resident of Virginia, a member of Washington Apple Pi, and the author of a slim volume called The Joy of Computer Communication, published by Dell in the fall of 1984. It is about how to make your personal computer talk on the telephone and all the wonders you can find on the other end of the line. In my real life I am a staff correspondent for Newsweek Magazine, though I am appearing here as a private individual. My wife and I have two sons, 13 and 15, and we share your concern about child pornography and the vicious people who purvey it.

I have been asked to talk briefly about computer communication. Huge mainframe computers have been able to talk to each other over special telephone lines for many years. But small privately owned computers which can communicate on the telephone are a very recent phenomenon, one still developing. As you all know, personal computers didn't start appearing in homes and offices until the very end of the 1970s, and they have only become common in the past three or four years. As part of the personal computer boom is a boomlet in personal computer communications.

It is quite easy and inexpensive to make a personal computer talk on the telephone. If you already have an Apple computer, a Commodore 64, an IBM personal computer, or a dedicated word processor such as a Wang, you need add only a modem and a special communications program. A modem, short for "modulator-demodulator," is a device that allows the technical connection between a computer and the telephone system. Since the telephone system is designed to carry voices, the modem converts the computer's electronic pulses into audible tones that it sings over the wire. Modems can cost as little as $60. Toy R Us, for example, sells modems for the popular Commodore computers. More sophisticated modems cost $200 to $500. A simple program -- some of them are free

-- sets up your computer to work with the modem, the telephone system, and a computer at the other end.

Personal computers that can communicate are enormously useful. If I choose to work at home on a Newsweek story, I can write it on my computer, then tell the computer to call Newsweek's computer in New York and send my copy at 1200 words a minute. I have an account in a Memphis, Tennessee, bank. I've given the bank a list of 23 people or companies to which I regularly pay bills. When I want to pay a bill, I simply tell the bank, via my computer, to sent Vepco, or C&P telephone, or the music teacher, a check for a certain amount.

This same useful technology is used for computer bulletin board systems. A bulletin board system is just what the name says it is, a small computer hooked to a telephone line that is used to pass messages back and forth, to publish short articles, and to send and retrieve public domain software programs. Most bulletin board systems are open to anyone who wishes to call, though you may have to apply for a password. A few charge modest fees. The first bulletin board systems appeared in 1978, set up so computer hobbyists could send programs back and forth by wire. No one knows how many bulletin board systems are in operation, for they come and go, but there are many thousands. When I researched my book in 1983 I estimated there were at least 1000 in operation; since then the number has exploded. I brought along one list of about 1000 bulletin board phone numbers that is published on a computer system.

Most bulletin boards are run for the fun of it by hobbyists. They already have a computer, they know they use it only an hour or two a day, so they run a BBS the rest of the time. Not all BBS's are just for fun. Some are operated by special interest groups like computer clubs. Some businesses are using bulletin boards as inexpensive electronic mail, online database, and message-handling systems.

There are a growing number bulletin boards run by businesses and government agencies. The National Bureau of Standards, for example, runs two of them. Goddard Space Flight Center runs a BBS dedicated to the get-away special packages that are launched by the Space Shuttle. Tysons Corner runs a BBS that you can call to find out about sales, movie times, etc. Some companies are starting to use bulletin boards as order-takers.

Operating your own BBS is not quite the modern-day equivalent of running a small community newspaper -- it's a whole lot easier to start a BBS and keep it going, for one thing -- but there are parallels. You become a center for communication. You can publish your views about anything, because it's your system. If you believe that information is power, you just may have a little more swat with your BBS running than you had before you set it up. At least, you may be invited to parties held by users of your BBS, regular occasions for some boards. The party-goers aren't just kids, either. "Young ones hang out on the system," one bulletin board in Atlanta told me, "but they can't come to the parties, because they're too young to drive."

The ability of literally anyone to set up a BBS is one of the wonders of both the technical age -- and the free society we live in. You can imagine what would happen if some kid in Moscow tried to set up a BBS with his Agat computer, a Soviet copy of the Apple II.

The equipment required to set up and operate a BBS can be very simple: a small computer, screen, a disk drive or two for storage, a modem, and a special computer program -- in all, for as little as a few hundred dollars. With that and a telephone line you -- the system operator or SYSOP -- are in business. Your computer will be able to accept phone calls from other computers automatically, 24 hours a day. You do not need to be around for the system to operate. If your board becomes

popular, there will be people calling it at all hours of the day and night.

Bulletin Board Systems come in many flavors, but typically they have files of information you can read if you wish, they have a messsage section, and they may have software -- computer programs -- that you can load into your own machine to use.

The stuff one finds on bulletin boards ranges from technical computer jargon to things for sale to simple-minded gossip. Dedicated computer hobbyists ask each other questions about their equipment and software. "I need help interfacing a NEC Spinwriter to an Apple using the CCS 7710 serial card. . . .Has anyone successfully interfaced the Apple/NEC at 600 Baud?" That cry for help went out on the BBS of Washington Apple Pi, the big Apple users club in Washington, D.C. A computer store BBS carried this personal message to (an apparently) young woman: "I think you're cute. How can I get a date with you?" The computer software that is available on bulletin boards is usually written by a computer owner who wants to share it with others. The programs can be about anything from income tax spreadsheet templates to a program I found once that made the IBM PC play bluegrass music.

There are bulletin boards dedicated to interactive fiction. One person starts a story and others carry it along, each writing a few paragraphs. Conventional literature is in little danger, however, of being overtaken by this new form.

And, of course, there are bulletin boards dedicated to getting people, usually but not always of the opposite sex, together. They are the functional equivalent of the ads in the back of the Washingtonian magazine. In the list of 1000 boards I mentioned earlier, there are about 40 boards that are sexually oriented. I talked to a 40-year-old divorced lady in Southern California who told me that she didn't want to try to meet people in bars, so she started calling computer bulletin boards. "When my husband and I split," she told me, "I let

people know I was single." Indeed, she said, she had two dates set up before her ex-husband had all his stuff moved out.

Bulletin boards are really simple and free versions of much larger, more complex computer-based mail and database operations. The Source, owned by Reader's Digest and located in McLean, has 60,000 subscribers. CompuServe, owned by H&R Block and located in Columbus, Ohio, has 235,000 subscribers who call in with their personal computers to send electronic mail, read the news, shop, and join special interest groups, including Veterinarians' Forum, where you can resolve your pet problems. Veterinarians' Forum would operate within CompuServe something like a freestanding BBS. There are also several big electronic mail operations, including MCI Mail, headquartered here in Washington, GTE Telenet, located in McLean, Tymenet, Omninet, Western Union, General Electric, and others. Some computer database operators, such as Lockheed Dialog, are adding electronic mail services. So far about the only commercial beneficiaries of bulletin board systems are the telephone companies which carry the calls. Telenet this summer decided to try to tap this growing BBS market, opening its packet-switched data network to those trying to call bulletin board systems long distance. For $25 a month you can make unlimited long distance computer calls on Telenet's PC Pursuit during nights and weekends.

When you start calling computer bulletin board systems, you enter a new and still developing technological subculture. You read a message, say, that asks a technical question. If you know the answer, you can write a paragraph. Sometimes you can strike up a letter conversation with someone you've never seen. You write a message, he responds in a day or two, you write back. You don't really know anything about the people who are writing the messages you are reading and replying to your messages except that they have a computer and, almost universally, they do not spell well.

Your computer pen pal may be anyone; you know only what he tells you. And he may not be who he says he is, for computers

offer splendid opportunities for fantasy. You can become anyone you want. For you are supplying all the cues on the other person's screen. There are, of course, lots of computer freaks. They want to learn more about their machines, and their conversations are not too different from those between ham radio operators. That would characterize much of the traffic on the Washington Apple Pi BBS.

Many of the people who use bulletin board systems are teen-agers, mostly but not entirely males. My two boys have never been very interested in making our computer talk on the phone, but they have friends who spend hours working the phones. Many of their friends would like to have modems, they say. I have a 12-year-old nephew in Houston who is hoping for modem in his Christmas stocking. These kids are just learning who they are in fact; they can have a wonderful time imagining they are someone else when they write messages back and forth.

Teenaged immaturity is compounded sometimes because computer communications in general often lack subtlety. First, most people do not type well, so they write cryptically. Second, they receive no feedback from the machine of the sort you get from others in conversation. Some studies have shown that computer messages are much more frank than face to face or phone conversations. Some even appear harsh, though the writer would probably not think of himself as a harsh person.

In other words, you have to be very cautious about interpreting what you read on a BBS. You person you see writing messages may be quite different from that person in fact.

Computerized bulletin board systems are easy to set up, they are proliferating, and, like newspapers, they can take many different forms and serve many different audiences. I would be happy to assist the committee in exploring their many uses.

Mr. WARRICK. What is a bulletin board system? Mr. Chairman, in order to understand the impact of S. 1305 on computer bulletin board systems, it is necessary to understand a little about how they work and how they are used.

We shall attempt to refrain from using the jargon that characterizes the computer industry. For reference, however, the following are a few terms commonly used to discuss computer bulletin board systems: BBS or CBBS: A computer bulletin board system, modem (MOE-dum): A device that converts the letters and numbers sent by a computer into tones that can be sent over regular voice telephone lines. "Modem" is a contraction of modulator-demodulator; SYSOP (SISS-op): A SYStem OPerator, a person who operates a bulletin board system. The term also applies to the person in charge of a large or mainframe computer.

Our perspective as people who operate bulletin boards is only slightly different. We would like next to address ourselves to the two principal parts of S. 1305 and explain why the bill in its present form would effectively put an end to computer bulletin board systems and many business enterprises that take advantage of computer communications.

S. 1305 in its current form would have the unintended effect of forcing the shutdown of many computer bulletin boards, electronic mail services and office computer networks. Because of the way computer bulletin board systems, electronic mail services, and office computer networks operate, making the transmission of obscenity of pornography illegal, would impose liability on innocent bulletin board system operators, businesses, and government agencies.

Mr. Chairman, the operative sections of S. 1305 in their present form all share a common characteristic: They make the transmission of obscenity and pornography illegal. Section 2 of the bill would make illegal "any obscene, lewd, lascivious, or filthy writing, description, picture, or other matter entered, stored, or transmitted by or in a computer." Similarly, section 3 of the bill would punish "[a]ny person who knowingly enters into or transmits by means of computer" information "for purposes of facilitating, encouraging, offering, or soliciting sexually explicit conduct of or with any minor, or the visual depiction of such conduct." Section 4 contains language similar to section 3. We understand, Mr. Chairman, that the intent of S. 1305 is: One, to punish the individuals who would, for example, use computers to further the sexual abuse of children, and two, to put out of business those who would make a living offering computer systems for the principal or exclusive use of those individuals who would engage in such conduct. In fact, S. 1305 would force the shutdown of virtually every bulletin board system in the country because the people who operate those systems will be at the mercy of the people who would abuse their systems.

Given the way computer bulletin board systems work, Mr. Chairman, the people who operate such systems would be at the mercy of anyone who called in. Someone with the purest of motives who took every reasonable precaution could nevertheless be convicted because of the act of a caller who, innocently or maliciously, left an obscene message on the bulletin board system.

To explain why this is so, Mr. Chairman, let us assume that you have made the modest investment in a personal computer and that you would like to set up a computer bulletin board system so that you can learn more about your computer and how to use it. Let us also suppose that you want to learn as much as possible, and so you have decided to let anyone who wants to call in do so. You would, incidentally, be typical of the majority of bulletin board systems in the country in this respect. Even for those bulletin board systems that restrict access to their BBS's, as Washington Apple Pi does, the number of people in the group will often be so large and membership so easy to come by that the board is for all practical purposes open to the public. If you were like most bulletin board system operators, you would let the bulletin board system program run all the time except for those few hours when you actually wanted to use the computer.

Now let us suppose that during the day while you were at work someone called your system and left an obscene message for everyone or a message soliciting child pornography. After this person left his message, the next caller who calls in would read the message. The reading of a message involves the transmission of that message from the bulletin board system computer to the second caller's computer—and the innocent bulletin board system operator has just committed a crime. As a practical matter, given the dozens of callers and hundreds of messages that come into a bulletin board system each day, it would be impossible for the system operator [SYSOP] of a board to watch every message as or just after it was entered—yet this is what the language of S. 1305 would require him to do in order to avoid criminal liability. The unintended result of S. 1305 would be to force operators to shutdown their systems.

One suggestion some have made is that a system operator could find out whether each of his callers is likely to engage in obscenity or pornography. This is impracticable, however. Most bulletin board systems are, as noted above, run by individuals as hobbies. These already-busy people are not able to conduct character reference checks on everyone who logs in or even everyone who applies for a password on a limited-access system. Moreover, even a character reference is not likely to tell if a person is likely to begin sending obscene messages—this is known only after the fact, after the bulletin board system's computer has transmitted the obscene message.

Even more frightening, Mr. Chairman, is the fact that, if S. 1305 is enacted in its present form, someone out to "do you in" could get you into trouble with the law by leaving on your bulletin board system an obscene message or a message soliciting sex with minors. An unscrupulous opponent of yours, Mr. Chairman, could call your bulletin board system, leave an obscene message, and when the next caller—Mr. Cook, from Newsweek magazine, let us say—calls in and reads the message, you are now a criminal because your computer has transmitted an obscene message to him. The law ought not to give someone else the power to make you a criminal.

Similarly, if someone were to want to play a prank or practical joke by leaving obscene or pornographic messages on your bulletin board system, you would be guilty of a crime, because under S.

1305 in its present form, a crime has been committed once the obscene or pornographic message is transmitted, regardless of the intent of the sender of the original message.

In addition to the effect on computer bulletin board systems, Mr. Chairman, S. 1305 in its present form would have an equally devastating effect on electronic mail, online information vendors and companies that link their computers together into networks. Electronic mail is used by many businesses and individuals for the immediate transmission of documents. The companies offering this service, such as MCI, Western Union, General Telephone and Electronics, and General Electric, perform a necessary and valuable service by guaranteeing the confidentiality of communications. Boone Pickens' electronic mail to his fellow investors, or General Motors' electronic mail to its field representatives asking about possible sites for its next automobile factory, would be extremely valuable information to many people. Unless MCI Mail can guarantee Mr. Pickens and General Motors that their messages will not be read by human eyes, they will not use electronic mail, and companies like MCI will be out of business.

Mr. Chairman, because S. 1305 puts the liability on the person or company transmitting obscene matter, companies like MCI will be forced to read every message in order to ensure that they were not breaking the law. It would not suffice to have a computer scan messages looking for key words, as anyone knowing what those words are or might be would be able to use circumlocutions to achieve the same effect. The law, quite properly, does not require the use of any particular set of words to constitute obscenity. The meaning in context is what counts, and that can be judged only by reading the message in context.

In addition, many messages with unintended double entendres would have to be delayed so that the company could conduct an investigation into the intent of the sender. Even if such a thing were practical, it would defeat the purpose of electronic mail. No company could offer electronic mail without exposing itself to grave risks if S. 1305 were enacted in its present form.

Another group that would be disrupted if S. 1305 were enacted in its present form is online database vendors. Some of these companies—for example, The Source, owned by Reader's Digest, and CompuServe, owned by H&R Block, run their own, highly sophisticated bulletin board systems and would be exposed to the same risks as small bulletin boards run by hobbyists. But these companies also make available from their vast computer banks to customers around the world billions of characters of data of information on thousands of subjects. These companies would be forced to review manually all of those data to make sure that there was no matter that might be considered obscene or pornographic. Section 2 of S. 1305 would make the storage of obscene matter illegal where a common carrier like a phoneline was used in connection with the obscene matter. This would mean that if S. 1305 were enacted, everyone with such information in their data banks on the date the law took effect would be breaking the law. Moreover, publishers of books that contain small amounts of obscene language, such as publishers of unexpurgated versions of the Watergate tapes, could be violating the law merely by storing the text for those books on a

computer. Even more bizarre is the fact that police departments with computer records of obscenity cases could themselves be breaking the law by transmitting those data to FBI computers.

The cost of this would be prohibitive, particularly for the companies that tend to offer information of interest only to specialists. A great many online database vendors of all sizes would be forced to go out of business along with bulletin board systems and electronic mail companies in order to avoid criminal liability—or even just the threat of negative publicity that would inevitably arise from a criminal investigation. This, too, would be an unintended, far-reaching effect on S. 1305 in its present form.

Finally, Mr. Chairman, many businesses and governmental agencies such as the Bureau of Labor Statistics link their microcomputers together in networks that allow those computers to exchange data and programs over datalines in very efficient, cost-effective ways. S. 1305 would cover such systems, as many of these datalines are part of the interstate telephone system or are connected to it in some way. Such datalines are therefore used in interstate commerce. S. 1305 in its present form would expose those businesses and Government agencies to criminal liability if someone put an obscene message on the network that was in turn transmitted to others. Like bulletin board systems, it would be virtually impossible to police such a system. And unlike bulletin board systems, where the computer program can tell who left the message, it is not always possible to tell who left what message on a computer network in an office or agency. A disgruntled employee, for example, could get his company into grave legal trouble by leaving a message soliciting children for explicit sexual conduct. Again, someone would be punished for conduct over which it had no control.

Mr. Chairman, another unintended effect of S. 1305 would be to make it illegal to operate a bulletin board system if you know that your system "is being used" to transmit obscene matter. The wording of the paragraph that appears at lines 4 to 8 of page 2 would mean that you, as a bulletin board system operator, would be breaking the law if someone called you and said,

> I have used your bulletin board system to leave obscene messages before and I am going to go on using it. Even if you delete my password, I will just log on under someone else's name and continue leaving obscene messages.

Nothing more would be needed to complete the offense: If you continued to operate your bulletin board system, you would be "knowingly . . . operat[ing]" a "computer program or service having reasonable cause to believe that [it] is being used to transmit" obscenity. Again, someone else would have the power to cause you to break the law—manifestly an unjust and un-American situation. Note also that under S. 1305's present wording, the computer service need not actually be offering obscene matter—only "reasonable cause to believe" is required. This problem, however, is easily solved by rewording the paragraph.

Another unintended aspect of S. 1305 in its present form is that sections 3 and 4 make no distinction between messages left by adults attempting to exploit minors and messages left by teenagers about themselves. A significant minority of bulletin board system

users are teenagers, usually teenage boys, at an age where they are discovering the opposite sex for the first time. If a teenager were to leave a message saying, "My name is Johnny Johnson, I am 16, and I am interested in making out with any girl I can find," that would constitute:

> Knowingly enter[ing] into or transmit[ting] by means of computer . . . any notice, statement or advertisement; or . . . any minors' name . . . for purposes of facilitating, encouraging, offering, or soliciting sexually explicit conduct of or with any minor . . . .

Johnny is now a criminal, and his computer equipment can be taken away from him under the forfeiture provisions of 42 U.S.C. 2253. What Johnny really deserves is a stern lecture from his parents on the propriety of such language in public—not criminal prosecution. Were an adult to leave a message advertising for Johnny to engage in such conduct, few Americans would hesitate to punish the adult, but it cannot be the intent of Congress to make Johnny a criminal for what is really a family matter. For the same reason, it is also unjust to make the bulletin board system operator criminally liable for Johnny's message when his computer transmits it to the next caller. This is discussed above.

One of the most interesting characteristics of using a bulletin board system as a means of public discussion is that a person comes across only in the words he or she chooses to use. Physical characteristics like race, sex, national origin, religion and age need not be disclosed to others unless the person leaving the message does so voluntarily—and even then there is no compulsion to be truthful. This is one of the most powerful advantages computer bulletin board systems have for people: Your ideas carry their full impact, and people cannot use your physical characteristics to give what you have to say short shrift.

But the other side of this valuable coin is that a person may not know the age of the person to whom he or she is sending messages. There have been a number of cases where people have met via a bulletin board system, fallen in love, and been married. While obviously those people did see each other in person before the ceremony, there is no way to keep, say, a teenage girl mature beyond her years from phrasing her messages so as to make another person think she is an adult who fully understands and desires "sexually explicit conduct" with the other person. Someone who suggested "sexually explicit conduct" to such a girl thinking she was a consenting adult capable of dealing with such a suggestion in a mature and responsible manner would, under S. 1305, be guilty of a crime notwithstanding his lack of intent to engage in such activity with a minor. The scienter requirement of section 3, as with the scienter requirement of the other provisions of S. 1305, is satisfied when a person knowingly enters a message. No knowledge that the message involves a minor is required under S. 1305 in its present form. Imposing criminal liability on someone for conversations on a bulletin board system, where it is virtually impossible to tell someone's true age, would be manifestly unjust.

Washington Apple Pi is most willing to assist the subcommittee in revising S. 1305 to eliminate these unintended effects. Mr. Chairman, we have been candid in our comments today about the effects of S. 1305 in its present form. We have pointed out many of the

shortcomings in the bill. We think, however, that it is the duty of anyone who would criticize something to offer to make it better. In the last few days, we have given much thought to specific changes that would prevent S. 1305 from forcing all bulletin board systems to close down while at the same time permitting S. 1305 to achieve those desirable goals that command broad support. So far, however, we have not been able to do so to our satisfaction, but we are willing to work with you, the other members of the subcommittee, and your staffs in that effort. Washington Apple Pi is an association of people familiar with microcomputers and how they work, and we also have a number of people who are familiar with the law and the legislative process. Mr. Chairman, Washington Apple Pi welcomes the opportunity to assist the subcommittee further in any way we can.

Thank you.

Senator TRIBLE. Mr. Warrick, I think we can work out those concerns and arrive at a product that will permit the law enforcement community to tackle the kinds of problems that we have heard about today.

Let me say, Mr. Minot, I want to reiterate my intention that this legislation be quite specific and underscore the need of criminal prosecutors to prove criminal intent. That is a very difficult thing to do. And I can tell you, I have wrestled with that as a criminal prosecutor, and our whole system is weighed against the prosecution, as it ought to be.

There is a heavy burden on the State or the Federal Government to prove its case beyond a reasonable doubt, and the whole premise of our system is that it is better to let 100 guilty men go free than one innocent man be convicted. It is not a perfect system, but a good system, and we are not going to do anything to undermine that system in this legislation. But with reference to your first point, you admit that there is a problem. You condemn these actions, and then you suggest that they ought to be more properly dealt with in an omnibus bill.

I would like to see a more comprehensive response to the host of computer crime problems we face. I would like to see our Federal laws updated, made to be more current with modern technology. That is why I have authored the bill, S. 440, that you have talked about. I can tell you that hearings will be held on that bill on October 30, and I would hope that we can move ahead with a more comprehensive approach. But absent that, I do not think we can ignore genuine problems when they exist, especially when we are talking about young people whose lives are being victimized. I am sure that on that premise we would agree as well, so I believe your testimony today has been quite constructive, and I would offer to you the opportunity to work with us in shaping this bill so that we can ensure that innocent folks are in no way affected by this legislation. The innocent citizen, the computer user, has nothing to be concerned about in this legislation, and I thank you very much.

Mr. WARRICK. Thank you, Senator.

Mr. MINOT. Thank you.

Senator TRIBLE. Last, but not least, we hear from Mr. Barry Lynn, who will testify on behalf of the American Civil Liberties Union.

Mr. Lynn is their spokesman on a number of issues, pornography among those.

Mr. Lynn, once again, I will say that your full statement will be made a part of the record, all 14 pages. You are invited to summarize that statement or you can read it in whole.

STATEMENT OF BARRY W. LYNN, ESQ., LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Mr. LYNN. With all due respect, Senator, to your sponsorship of this bill, I find the very title of the bill somewhat misleading, in that it suggests that this legislation will substantially ameliorate the sexual exploitation of children.

If upheld by the courts, this bill, considered in its entirety, will primarily terminate services which now permit consenting adults to communicate privately via home computers about their sexual thoughts and fantasies. It is not primarily a vehicle for ending child abuse, and in fact would be unlikely to make any real contribution in that area.

ALLEGEDLY OBSCENE MATERIAL

S. 1305 would amend 18 U.S.C. 1462, which now bars importation of certain forms of obscene material, to include "any obscene, lewd, lascivious, or filthy writing, description, picture, or other matter entered, stored, or transmitted by or in a computer." It also seeks to penalize anyone who "knowingly owns, offers, provides, or operates any computer program or service having reasonable cause to believe" it is used to transmit such described material.

The Supreme Court has carved out several exceptions from the first amendment for certain forms of sexually oriented speech. In 1957, the Court in *Roth* v. *United States* 354 U. S. 476 (1957) held that obscenity, at least in some contexts, was not entitled to constitutional protection. In *Miller* v. *California* 413 U.S. 15 (1973) obscenity was defined to encompass material which: (1) "appeals to the prurient interest" as judged by the average person applying "contemporary community standards," (2) "describes or depicts, in a patently offensive way" specified sexual conduct defined by statute, and (3) which taken "as a whole * * * lacks serious literary, artistic, political, or scientific value." It is no secret that the ACLU does not approve of these decisions. We believe that sexual speech does have certain ideas, albeit frequently offensive ones graphically disseminated, which ought to be accorded constitutional protection. Likewise, the standards in *Miller* are hopelessly vague and overbroad, casting a chill on sellers, producers, and distributors who need to fear that particularly sensitive or particularly zealous persons will be offended and seek legal recourse.

The ACLU takes no position on the quality or social utility of speech, pornographic or otherwise. We believe that all speech even the often offensive messages in computer pornography are protected by the first amendment. Rational discourse specifically designed to educate is not the only speech protected by the guarantees of free expression.

The Supreme Court recognized the significance of nonrational expression in *Cohen* v. *California* 403 U.S. 15, at 26 (1970) where it

assessed the impact of Cohen entering the trial court wearing a jacket emblazoned with the words "Fuck the Draft": "[M]uch linguistic expression serves a dual communicative function: it conveys not only ideas capable of relatively precise, detached expliction, but otherwise unexpressible emotions as well. In fact, words are often chosen as much for their emotive as their cognitive force. We cannot sanction the view that the Constitution, while solicitous of the cognitive content of individual speech, has little or no regard for that emotive function which, practically speaking, may often be the more important element of the overall message sought to be communicated * * *."

Likewise "speech" interests may extend even to exotic nude dancing: "[E]ntertainment, as well as political and ideological speech * * * fall[s] within the first amendment guarantee" *Schad* v. *Borough of Mount Ephraim* 452 U.S. 61, 65 (1981) (citations omitted).

This is not the forum, however, in which to rekindle the battle over obscenity law as such. Therefore, I would like to focus on why even *Miller* would not permit the broad intrusions into the distribution of sexually-oriented material via computers sanctioned by S. 1305.

ADULT COMPUTER SERVICES

A number of commercial services presently exist which permit a subscriber to have access to databases and other communication facilities in which sexually-oriented material is available. The following description is generic, but covers the essential mechanics of most of these services.

A potential subscriber learns of the service through an advertisement in a sexually-oriented adult magazine. When he writes for information, he is sent a description of the service, along with a membership form. The form requires a certification that the subscriber is over 18, along with credit card data (the only way in which charges may be billed) and request for a user password.

Once the application is processed, the subscriber receives more complete explanatory information and a phone number to call to link up the system. The subscriber gets access to the service by hooking up his computer and telephone to a modem and dialing the service telephone number. He then enters his account number, credit information, and password. A "menu" appears which provides topical listings such as "adult film reviews," "bulletin boards," "personals," and "conferencing." "Bulletin boards" and "personals" usually contain notices of interest to subscribers or requests to meet individuals with specific interests, sexual or otherwise. Teleconferencing permits a subscriber not merely to look at posted notices, but to type out messages to other persons presently using the service. He can page persons interested in writing about specific sexual topics or join existing written dialogs. Most services contain a method for blocking or gagging interlopers if two or more persons wish to maintain the privacy of their conversation. It is my understanding that some of these services periodically monitor at least their bulletin boards to remove material which does not meet their publishing standards or guidelines.

The ACLU does not believe that these services should be regulated. In our view, sexually oriented communications via computer cannot and should not be prohibited. In *Stanley* v. *Georgia* 394 U.S. 557 (1969), the Supreme Court held that even obscene material may be viewed in one's own home: "If the first amendment means anything it is that a State has no business telling a man, sitting alone in his own house, what he may read or what films he may watch."

Stanley is clearly applicable to conduct which consists of simply entering or storing obscene communications. If you can read an obscene book in your home under *Stanley,* you can certainly write one there, whether with a pen on a yellow pad or with a word processing program on your computer screen.

Admittedly, the Supreme Court has held that the privacy interest in the home does not mean that all means of distribution are also protected (see, for example, *United States* v. *12 200 Ft. Rolls of Film* 413 U.S. 123 (1973)). However, it is also true that even computer-based material which is transmitted is distributed quite differently than books, 8-millimeter films, and motion pictures in theaters. *Miller* notes that "these specific prerequisites—the three-prong test—will provide fair notice to a dealer in such materials that his public and commercial activities may bring prosecution" Id. at 27. Although adult computer services have a commercial purpose, they cannot reasonably be labeled public. Actual communication between parties is facilitated by an automated, electronic switching system which does not generally involve a third party.

Even if one does not accept the premise that "computerized pornography" is not covered by *Miller,* there is certainly no requirement in *Miller* that every new form of communication be regulated as extensively as already existing forms. There is absolutely no evidence of any adverse effect caused by two adults typing out sexually-explicit messages. Even social science data which alleges that exposure to certain pornography exacerbates negative attitudes or contributes to antisocial laboratory conduct uses visual material considerably more graphic than the words on computer screens. The Congress needs to make a judgment about whether the new computer technology should be saddled with the moralistic regulation of older technologies. Obviously, some of the talk over computers is hardly the kind of conversation we would find appropriate in this hearing room or in our homes. However, this talk is not intruding upon these places; it is confined to the privacy of two people's computer terminals.

It is clear that the right of free expression may be balanced against a right of personal privacy under some circumstances, particularly in regard to the so-called unwilling listener. Where this conflict in fact exists, "the right to be left alone must be placed in the scales with the right of others to communicate." *Rowan* v. *Post Office Department* 397 U.S. 728, 736 (1970). However, voluntary use of adult computer services intrudes upon no privacy rights of others. There are absolutely no unwilling participants. It is the quintessential example of the right to privately receive information and ideas. The service can be accessed only by the complex, affirmative act of a voluntary participant who has clear knowledge of what he or she is about to view.

Every reasonable effort is made to keep children out of these systems. The services are advertised primarily in publications not sold to minors, membership applications are not accepted from those who do not certify they are over 18, and, most importantly, all billing is done through credit cards which are rarely issued to minors. In all systems of which I am aware, even were a minor to find the telephone number and his father's credit card, that minor would still need a password known only to the actual subscriber. Of course, no one can guarantee that no minor will ever tap into a computer sex service, but the first amendment commands that protection of children not become a catch-all justification for the curtailment of the rights of adults. As Justice Frankfurter noted for the Court in striking down a statute which prohibited the sale of books "tending to the corruption of the morals of youth," the risk it presented was "to reduce the adult population to reading only what is fit for children." *Butler* v. *Michigan* 352 U.S. 380 (1957).

In addition, the intended reach of section 2 is astounding. Anyone who "owns, offers, provides, or operates" an interstate program or service who has "reasonable cause" to believe it is involved with obscene communication is liable for extraordinarily stiff penalties. This is like prosecuting a letter carrier with a Federal crime for delivering Hustler magazine because some courts have considered some issues of the magazine obscene.

In the context of this new technology, just what does a reasonable cause standard mean? The bill essentially charges everyone from the telephone company to large multiservice database owners to noncommercial operators of small electronic bulletin boards with a responsibility to scrutinize the communications they are somehow facilitating. If a bulletin board or service has the word "sex" in it, is one presumed to be reasonably aware of its possibly obscene contents? Is a company which operates a personals or teleconcerencing service responsible to monitor each communication? Since many juries and Federal judges have had difficulty applying Miller for 12 years, how are bulletin board operators supposed to assess their contents? There is a substantial possibility that anything related to sex will be barred from computer communication. This is the essence of a chill on constitutionally protected speech—that persons will not communicate about sexual matters at all because of the concern that the FBI will listen in and swoop in on them for providing a service which somebody finds potentially obscene.

The ACLU policy on child sexual exploitation and pornography: The American Civil Liberties Union views the use of children in the production of visual depictions of sexually explicit conduct as a violation of children's rights whenever such use causes substantial physical harm or continuing emotional or psychological harm. Governments, including the Federal Government, quite properly may take action to protect the interests of children in these situations by the use of criminal prosecution of these persons who are likely to cause such harm to children. These persons are usually those who finance the sexually explicit depictions, those who procure the children, and those who engage in sexual activity with the children. Nevertheless, we oppose statutes which restrict the distribution of any printed or visual materials themselves even where

some or all of the producers of the material are punishable as noted above. The first amendment protects only dissemination of communication; it does not insulate actual sexual abuse from the reach of the criminal law.

Regrettably, several provisions of S. 1305 run afoul of the first amendment. Moreover, they do not carefully track extant Supreme Court precedent on vagueness and overbreadth, seeking to cover far more activity than that which is collateral to actual sexual exploitation. Finally, even if some provisions would withstand judicial scrutiny, the whole statute addresses a problem of miniscule proportion in comparison to the growing and serious threats to the rights of children which go largely unpunished. Cleaning up dirty pictures or scrutinizing the fantasies of disturbed individuals is not a meaningful approach to the growing problem of child sexual exploitation.

Computers and child abuse: Section 3(c) of S. 1305 would amend 18 U.S.C. 2251 to penalize "any person who knowingly enters into or transmits by means of computer * * * any notice, statement, or advertisement; or any minor's name, telephone number, place of residence, physical characteristics, or other descriptive or identifying information, for purposes of facilitating, encouraging, offering, or soliciting sexually explicit conduct of or with any minor, or the visual depiction of such conduct * * *" It has an extraordinarily wide coverage, however. Even legislation with a constitutional purpose, through too broad a sweep, may become unconstitutional. See *Graynard* v. *City of Rockford,* 408 U.S. 104, 114 (1972). This provision is presumably designed to combat child abuse. According to the statement of S. 1305's primary sponsor, Mr. Trible, this provision is needed because "the computer also seems to have become a preferred method of communication among child molesters," Congressional Record, S 8242 (June 17, 1985). Outside of a smattering of anecdotes, there is a dearth of evidence to support this theory of the preferred use of computers by pedophiles. Most of the illustrations cited by Mr. Trible involve use of computers to either catalog sexual activity or pornography collections or maintain mailing lists. In fact, Mr. Trible has indicated that one major purpose of this legislation is to deter the pedophile use of computers "to catalog information about their victims," Congressional Record, S 8241 (June 17, 1985). Obviously this chronicling could be done with index cards rather than computers. Whether entered onto three by five cards or computer disk, the mere filing of this information, no matter how repugnant, cannot define a new Federal offense. Surely, a bank robber who writes about his crime spree cannot be charged with another crime consisting merely of reporting about his activities.

There is another irony to this approach. In most reported cases of pedophile computer use the prosecution of underlying sexual assaults was apparently enhanced by evidence obtained through examination of information contained in computer files. Were the defendants not such meticulous chroniclers of their crimes, their offenses against children might have gone undiscovered. [The ACLU does not necessarily endorse every investigatory technique used in the prosecution of such cases. We believe that undercover oper-

ations should be conducted based on probable cause that an identified individual has committed a criminal offense.]

Even if the language was clarified or modified to cover only the transmission of the proscribed descriptions, the section would not withstand constitutional scrutiny. A student who runs a northern Virginia teenager dating service may transmit records with identifying information about possible clients. Since, occasionally, persons who date may engage in sexual activity, could the dating service operator be charged with the purpose of encouraging, or at least facilitating sex with a minor? If an electronic bulletin board contains a message which urges change in child sex laws to permit sexual activity with minors—not a position endorsed by the ACLU—would this advocacy be deemed encouragement to sexual conduct because it tends to legitimize, or validate such conduct? In our view, the activity described in these examples is fully protected by the first amendment, yet is covered by the statutory language. An intent requirement covering purposes of facilitating, encouraging, offering, or soliciting sexual conduct is far too imprecise. To attempt to bar publication oi the physical description of a minor because it might somehow encourage sexual activity even with an entirely different child is hopelessly vague.

Such an oblique intent does not meet incitement standards in *Brandenburg* v. *Ohio* 395, U.S. 444 (1969)—speech may be punished where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action—or even the solicitation standards in *Hoffman Estates* v. *Flipside,* Hoffman Estates, 455 U.S. 489 (1982)—"speech proposing an illegal transaction * * * government may regulate or ban entirely.") S. 1305 is no narrowly drawn statute which simply prohibits use of a computer to plan a criminal enterprise such as the kidnaping of an identified child.

Advertising child pornography: There is no evidence that child pornography as defined in the existing Child Protection Act, 18 U.S.C. 2251, is distributed by computer. The act regulates only the actual visual depiction of sexually explicit conduct actually involving minors, not any description of sexual activity with minors. Section 4 of S. 1305 amends the act to prohibit certain publications and distributions of any notice, statement, or advertisement to buy, sell, receive, exchange, or disseminate any visual depiction, if the producing of such visual depiction involves the use of a minor engaging in sexual explicit conduct and such visual depiction is of such conduct. Leaving aside the reasons for our opposition to much of the reasoning in *United States* v. *Ferber,* 458 U.S. 747 (1982) this section does not really contribute to enhanced law enforcement of the "child pornography" statute.

To prove this proposed advertising offense requires proof of essentially the same elements as the existing statute. Advertisements in recent copies of some adult magazines suggest that the advertisers have material portraying young women in sexually explicit poses. S. 1305 does not prohibit their ads, per se, nor could it under the first amendment. Unless one can prove that the photographs offered are indeed of a minor, and not an 18-, 21-, or 30-year-old dressed up or posed to look like a minor, there is no violation of the statute. This proof could only be obtained after purchase of the

advertised material. Since a U.S. attorney is going to have to produce the material in order to prove that a model is indeed a minor, he or she might as well prove it for purposes of prosecution for sale or other distribution of child pornography.

Conclusion: S. 1305 is a hopelessly flawed proposal which should not be enacted. Consensual sexual communication between adults should not be regulated. Child sexual exploitation should be penalized through narrowly drawn statutes which proscribe conduct rather than expression.

Senator TRIBLE. I welcome your concern about actions that we might undertake that would in any way compromise the ability of the law enforcement community to do its job.

Mr. LYNN. I think that is an area that we should all be willing to explore.

Senator TRIBLE. That is a striking position for you to take, and I welcome that statement.

Mr. LYNN. We have spent a great deal of time at the ACLU trying to make it clear that the first amendment covers a lot of material and still does not protect people who finance child pornography, or who abuse children. It protects the dirty books that might be products. Even if this bill was covering only the described transmission, I do think there is an additional constitutional overbreadth problem. There is, as you may have seen in northern Virginia newspapers, at least one teenager who runs a computer dating service. Since occasionally persons who date have been known to engage in sexual activity, could the dating service operator or be charged with the purpose of encouraging or at least facilitating sex with a minor. I think under this language the clear answer is yes.

In our view, that activity described in this example is fully protected by the first amendment, no matter how repulsive, yet is covered by statutory language. It is just too imprecise and oblique a standard. The bill is not narrowly enough drawn. Let me just end this way. There is a third section of this bill dealing with the advertisement of child pornography. I find it difficult to believe that that would be of much use in the enhancement of law enforcement. To prove this proposed advertising offense requires proof of essentially the same elements that are now in existing child protection statutes.

Since the U.S. attorney is going to have to produce the material in order to prove that a model is indeed a minor, then that U.S. attorney might as well prove it for purposes of production for sale, rather than some new advertising offense that might be created in this bill.

I thank you for the opportunity to testify.

Senator TRIBLE. Mr. Lynn, the position of the ACLU is quite predictable, but I welcome your testimony today. And obviously, it will be considered by the committee. Suffice it to say that in the area of expression, the position of the ACLU is, simply put, everything goes. Fortunately, that is not the position of the Supreme Court. That is not the position of the witnesses that we have heard today, and it is clearly not the position of the American people.

Mr. LYNN. If I may correct you slightly, it is not, I think, an accurate assessment in all areas of what the ACLU believes. We have

urged at other times, and here today, that narrowly drawn solicitation statutes may pass constitutional muster, but this particular bill simply in our view does not meet those narrowly drawn standards.

Senator TRIBLE. With that, we will conclude your testimony.

This hearing is brought to a close. Thank you.

[Whereupon, at 12:20 p.m., the subcommittee adjourned, subject to the call of the Chair.]

APPENDIX

Additonal Statements and Views

STATEMENT OF THE AMERICAN SUNBATHING ASSOCIATION, INC.
TO THE SUBCOMMITTEE ON JUVENILE JUSTICE,
COMMITTEE ON THE JUDICIARY, UNITED STATES SENATE
November 6, 1985

The purpose of this statement is twofold: (1) to relate some brief general information about the standards and practice of social family nudism today, and (2) to share some concerns about recent efforts to curb certain types of pornography regarded as harmful to children, or subject matter which appeals to those who might exploit them.

We would like to begin by telling you a little about the American Sunbathing Association.

Modern social nudism generally traces its beginnings to turn-of-the-century Germany where freikorperkultur ("free body culture") parks were established with emphasis on outdoor physical conditioning in a sometimes harsh climate, vegetarianism and clean living. Caffeine, tobacco and alcohol were taboo. This history, with its air of self-justification, is responsible for some modern day jokes and unfortunate perceptions of nudists as a cult carrying on activities in semi-secret "colonies." Fortunately, this image is changing as people recognize it as a legitimate choice of living style or preferred adjunct to recreation.[1]

The movement came to America in 1929 and in 1931 the nonprofit American Sunbathing Association, Inc. was founded and continues as the chief spokesman for what is now an expanding recreation interest. Headquartered with a small professional staff in Kissimmee, Florida, the ASA has over 30,000 members through some 200 clubs in North America. It is affiliated with the International Naturist Federation, in Antwerp, Belgium.

Nudity in bathing, sunbathing and recreation is, of course, no modern invention, nor was it dependent on introduction from abroad. America's second President regularly bathed nude in the Potomac, and some 19th Century communities, such as Home, Washington, made formal provision for nudity.

More recently, in 1980 the Naturist Society was founded in Oshkosh, Wisconsin to focus the interest of the much larger phenomenon of so-called free beaches and similar expression of more purely recreational use of public lands, secluded areas, hot springs and traditional areas long used for "skinny dipping." Some, like Black's Beach near San Diego, California, have become as famous as they are popular, similar to the growth which has occurred in the Europe's Mediterranean resort playgrounds.[2]

A Gallup poll conducted in 1983 not only showed a 74 percent majority acceptance of nude recreation, but indicated that 15 percent of the survey respondents themselves had already experienced it.[3]

From its very beginnings, the nudist movement had been a family oriented philosophy. Belief in the fundamental wholesomeness of the human body extends to people of all ages. We believe that the ability to realize this special form of freedom facilitates a healthy outlook on life, one which eliminates the more common connection others make between nudity and sex. We find this philosophy, and its natural acceptance of basic human worth of each individual, to be of special value to growing children. As one non-nudist investigator concluded:

> [N]udist children may have an advantage over a great many other children in our culture who have never been exposed to the same or opposite sex in the nude. We view this as a positive aspect of nudism, for both the children and adults. It not only gives children the opportunity to see that they are like other boys and girls, but it gives the parents the opportunty to notice that Johnny and Jane are developing at about the same maturation rate as the other youngsters their age.[4]

In American law, nudity is not equated with obscenity.[5] Our courts have wisely followed a course of defining the offensive in

terms of sexually overt actions, e.g., "lewd exhibition of the genitals," "exhibition calculated to offend or affront," and the like.[6] We view this long-accepted distinction to be critically important to the understanding of our lifestyle and to the protection of our children, their health and well-being.

If, by error or zeal, the distinction between "nude" and "the lewd" were to be ignored, the "body taboo" believed in by others would begin to seem real to our children, threatening the healthy outlook we prize so highly.

Social nudism as practiced within the ASA provides a wide range of activities for all ages. Athletics, social recreation, and interpersonal communication promote the betterment of body and mind and strengthen family bonds.

We believe the wholesome photographic and electronic portrayal of the nude form is essential to the education of the general public and the documentation of the nudist movement. We believe that this includes the inherent right to photograph and portray our children enjoying the nudist lifestyle whether the setting be a nudist park, beach or home. Within the ASA nudists have standards and regulations in regards to photography. It is our purpose to educate and differentiate between this legitimate nudist photography and that which we deplore: the exploitation of children as objects of pornography or violence.

But problems have been encountered stemming from two general areas of misunderstanding. The first has its genesis in widely adopted state statutes requiring commercial photo processors to report suspect photography to appropriate authorities.[7] While it has generally been our experience that both photo processors and law enforcement personnel are fairly well acquainted with innocent nude photography, there have been regrettable instances of harassment, questioning and initial charges (later dismissed) over pictures taken at nudist resorts and nude beaches.

The second and potentially more serious is an apparent misunderstanding of the U. S. Supreme Court's holding in New York

v. Ferber.[8] Lawmakers and others seem to think that because the broad message of Ferber is that states will be allowed more latitude in regulating obscenity which uses and exploits children than the "hard core" standard established for adults in Miller v. California,[9] they are free to engage in virtually any regulation including that which goes to simple nudity. It is not the purpose of this position paper to delve deeply into the developed law in this area. The Committee's staff is well qualified to advise on those points. Suffice to say, the Ferber Court took care to aim at only the subject which is sexual in its content, both as to the images and the intended audience.[10]

The Court reiterated approval, accompanied by the cautionary concurring opinions of Justices O'Connor[11] and Stevens, of its own standing rule established in Erznoznik v. City of Jacksonville that "nudity, without more, is protected expression, 422 U.S. 205 at 213."[12] Further, it is readily apparent that the materials at issue and the focus of the New York law which was upheld, are confined to "hard core" child pornography.[13]

For these reasons we express our concern and disagreement with broad-brush lawmaking illustrated by Ohio's recent attempt to outlaw portrayals of "a child in a state of ..udity."[14] The American Sunbathing Association is now seeking to participate as amicus curiae in the appeal of a trial court decision declaring that statute unconstitutional. (Copies of the statute and the trial court's opinion in State v. Robinson are attached.) Without a modification of the statute, the mailing of our monthly newspaper The Bulletin, (sample copies of which have been supplied to you along with some other of our informational materials) which goes to members and supporters all over North America, is a fourth class felony in Ohio.

This Committee may make recommendations, findings, and formalized reports for consideration by the Congress and other agencies. We solicit appropriate findings supporting the principle that nudity is not obscene. Not only would this constitutionally

and historically established point be worth repeating, but elimination of actual or potential confusion in such a direct way would aid the law enforcement and theraputic professionals by providing a distinction which allows focus on the real evils of violence, abuse and exploitation. Such a clarification would hopefully obviate situations such as Ohio's attempt to presumably deny access to materials found stimulating to a small minority of sick individuals, which then tramples upon other well-established rights.

The fact is that nude (or even many clothed) portrayals of children are appealing to pedophiles. So, it seems, are their voices, stories, diaries and juvenile clothing ads.[15] Neither the Congress nor state legislatures can, or should, attempt to control the existence or publication of material which clearly constitutes protected expression, whether in a simple family snapshot or a great work of art. Such prohibitions would not only be wrong as a matter of law, but doomed to failure.[16] The abolitionist approaches divert attention and resources from the tried and true methods available to law enforcement to get at the root of problems of exploitation of children.[17]

Our organization remains dedicated to the welfare of our present and future adherents and especially to our children. In no sense would we wish to be seen as ignorant, let alone tolerant, of any form of sexual exploitation of a child. We believe that the protection of our freedom to express our principles and standards[18] strengthens everyone's ability to distinguish the open, joyful and natural portrayal of body freedom from any form of degradation.

Finally, we feel that great care must be exercised before any recommendation or lawmaking occurs which would in any way censor such normal expressions of body freedom as are enjoyed in family homes, the old swimming hole and the like, regardless of any connection to organized interests such as ours. The nearly universal experience of innocent nudity cannot be quelched just because its portrayals appeal to some child abusers as well.

The American Sunbathing Association is grateful to the Committee and its staff for the opportunity to present these views. We stand ready to assist in any reasonable way with your fact-finding efforts.

FOOTNOTES

[1]See, Goodrich, "Skinny Dipping: The Old Swimming Hole Breeds New Controversy," 15 Parks & Recreation, No. 5, 33 (May 1980).

[2]L. Baxandall, World Guide to Nude Beaches and Recreation (Crown 1983) 220 pp.

[3]Press release describing survey composition and results attached.

[4]W. Hartman, et al., Nudist Society 130-31 (Crown 1970).

[5]Erznoznik v. City of Jacksonville, 422 U.S. 205 (1975); Jenkins v. Georgia, 418 U.S. 153 (1974); Sunshine Book Co. v. Summerfield, 355 U.S. 372 (1958); New York v. Ferber, 458 U.S. 747, 765-66 at n.18 (1982); HBO, Inc. v. Wilkinson, 531 F. Supp. 987 (D. Utah 1982).

[6]United States v. Various Articles of Obscene Merchandise, 460 F. Supp. 826, 830 (S.D.N.Y. 1978).

[7]E.g., California Penal Code §§11165-66.

[8]458 U.S. 747 (1982).

[9]413 U.S. 15 (1973).

[10]458 U.S. 747, 764-65.

[11] "On the other hand, it is quite possible that New York's statute is overbroad because it bans depictions that do not actually threaten the harms identified by the Court. For example, clinical pictures of adolescent sexuality, such as those that might appear in medical textbooks, . . . might not involve the type of sexual exploitation and abuse targeted by New York's statute. Nor might such depictions feed the poisonous "kiddie porn" market that New York and other States have attempted to regulate. Similarly, pictures of children engaged in rites widely approved by their cultures, such as those that might appear in issues of National Geographic, might not trigger the compelling interests identified by the Court." 458 U.S. 747, 775 (O'Connor, J., concurring).

[12]"Nor will we assume that the New York courts will widen the possibly invalid reach of the statute by giving an expansive construction to the proscription on 'lewd exhibition[s] of the genitals.'" Id. at 773.

[13] Id. at 751.

[14] Ohio Rev. Code §2907.323.

[15] See, Statement of Kenneth V. Lanning, Behavioral Science Unit, Federal Bureau of Investigation, to the Subcommittee on Juvenile Justice, U.S. Senate Committee on the Judiciary, Hearings, Effect of Pornography on Women and Children 38 (August 8, 1984).

[16] Statement of John Money, Ph.D., Professor of Psychology and Pediatrics, Johns Hopkins University School of Medicine, Id. at 338 (October 30, 1984).

[17] Id. at 340-342.

[18] "We believe in the essential wholesomeness of all human bodies and of the natural functions and activities which they perform. We believe in the naturalness of social nudism and we consider that exposure of the entire human body to sun, light and air is beneficial. We believe that we have the right to practice social nudism, provided that we do not infringe upon the rights of others." ASA, Principles and Standards (1931).

PRESS RELEASE

For Immediate Release

Contact: Susan A. Weisbrod,
The Gallup Organization,
Princeton, New Jersey

Gallup Poll Finds -

Most Americans Approve of Nude Recreation

Should people be free to enjoy nude sunbathing without interference by officials as long as they do so at beaches that have found acceptance for that purpose? Some 72% of Americans answer "Yes", according to a survey conducted by The Gallup Organization for The Naturist Society of Oshkosh, Wisconsin and released today.

The nationally representative study found higher approval among younger adults (ages 18-29) and the better-educated segment of the population (with at least some college) than among older adults (age 50 and over) or those with less than a high school education. Also, more men (80%) state approval than do women (65%).

Not only do most American adults accept nude sunbathing but 15% have themselves "skinnydipped" in a mixed group, according to the Gallup poll. (In the American western region, 23% have done it.) Only 5% of older adults have participated while 24% of the 18-29 age group have joined other men and women in nude bathing.

Significantly fewer adults (39%) out of the entire population sample say they believe the government should set aside public lands specifically for nude sunbathing. 54% are opposed, and 7% say they "don't know." The group most approving of nude sunbathing - the 18 to 29 year olds - is about evenly divided on the government set-asides.

The telephone interviewing of representative survey of 1,037 was conducted between May 13 and May 30, 1983. The margin of error is plus or minus four percentage points, the Gallup Organization said.

#####

(For exact wording of the questions asked: See reverse.)

Gallup Poll Survey of Attitudes on Nude Sunbathing, Conducted May 1983 '

1. Do you believe that people who enjoy nude sunbathing should be able to do so without interference from officials as long as they do so at a beach that is accepted for that purpose?

MEN: "Yes" 79.5% "No" 15.2% "Don't Know" 5.3%
WOMEN: "Yes" 64.7% "No" 31.5% "Don't Know" 3.8"

TOTAL POPULATION:
"Yes" 71.6%
"No" 23.9%
"Don't Know" 4.5%

AGE 18-29: "Yes" 86.0% "No" 11.4% "Don't Know" 2.6%
AGE 30-39: "Yes" 77.4% "No" 18.9% "Don't Know" 3.7%
AGE 40-49: "Yes" 73.1% "No" 21.9% "Don't Know" 5.0%
AGE 50 AND OVER: "Yes" 59.1% "No" 35.0% "Don't Know" 5.9%

LESS THAN HIGH SCHOOL GRAD: "Yes" 52.6% "No" 40.6% "Don't Know" 6.7%
HIGH SCHOOL COMPLETE: "Yes" 73.5% "No" 22.3% "Don't Know" 4.2%
COLLEGE: "Yes" 82.5% "No" 14.2% "Don't Know" 3.4%

INCOME LESS THAN $10,000: "Yes" 60.5% "No" 36.3% "Don't Know" 3.1%
INCOME $10,000 TO $19,999: "Yes" 71.2% "No" 25.2% "Don't Know" 3.6%
INCOME $20,000 TO $29,999: "Yes" 77.3% "No" 16.8% "Don't Know" 5.9%
INCOME $30,000 AND OVER: "Yes" 80.8% "No" 16.9% "Don't Know" 2.3%

EAST REGION: "Yes" 76.8% "No" 21.1% "Don't Know" 2.1%
CENTRAL REGION: "Yes" 69.7% "No" 24.1% "Don't Know" 6.2%
SOUTH REGION: "Yes" 64.7% "No" 28.5% "Don't Know" 6.7%
WEST REGION: "Yes" 78.3% "No" 19.9% "Don't Know" 1.8%

2. Have you personally ever gone 'skinnydipping' or nude sunbathing in a mixed group of men and women either at a beach, at a pool or somewhere else?

MEN: "Yes" 20.6% "No" 77.8%
WOMEN: "Yes" 9.5% "No" 88.3%

TOTAL POPULATION:
"Yes" 14.7%
"No" 83.4%

AGE 18-29: "Yes" 23.9% "No" 74.5%
AGE 30-39: "Yes" 23.2% "No" 73.1%
AGE 40-49: "Yes" 11.9% "No" 85.4%
AGE 50 AND OVER: "Yes" 4.9% "No" 94.6%

LESS THAN HIGH SCHOOL GRAD: "Yes" 9.9% "No" 89.2%
HIGH SCHOOL COMPLETE: "Yes" 10.1% "No" 87.3%
COLLEGE: "Yes" 23.4% "No" 74.9%

INCOME LESS THAN $10,000: "Yes" 9.0% "No" 90.1%
INCOME $10,000 TO $19,999: "Yes" 14.4% "No" 83.8%
INCOME $20,000 TO $29,999: "Yes" 17.4% "No" 80.6%
INCOME $30,000 AND OVER: "Yes" 19.2% "No" 79.7%

EAST REGION: "Yes" 15.7% "No" 81.7%
CENTRAL REGION: "Yes" 10.8% "No" 86.9%
SOUTH REGION: "Yes" 12.1% "No" 86.7%
WEST REGION: "Yes" 23.2% "No" 75.4%

3. Local and state governments now set aside public land for special types of recreation such as snowmobiling, surfing, and hunting. Do you think special and secluded areas should be set aside by the government for people who enjoy nude recreation?

MEN: "Yes" 47.6" "No" 46.2%
WOMEN: "Yes" 31.5% "No" 60.1%

TOTAL POPULATION:
"Yes" 39.1%
"No" 53.9%

Ohio Rev. Code

[§ 2907.32.3] § 2907.323 [Illegal use of minor in nudity-oriented material or performance.]

(A) No person shall do any of the following:

(1) Photograph any minor who is not the person's child or ward in a state of nudity, or create, direct, produce, or transfer any material or performance that shows the minor in a state of nudity, unless both of the following apply:

(a) The material or performance is, or is to be, sold, disseminated, displayed, possessed, controlled, brought or caused to be brought into this state, or presented for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial, or other proper purpose, by or to a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or research, librarian, clergyman, prosecutor, judge, or other person having a proper interest in the material or performance;

(b) The minor's parents, guardian, or custodian consents in writing to the photographing of the minor, to the use of the minor in the material or performance, or to the transfer of the material and to the specific manner in which the material or performance is to be used.

(2) Consent to the photographing of his minor child or ward, or photograph his minor child or ward, in a state of nudity or consent to the use of his minor child or ward in a state of nudity in any material or performance, or use or transfer such material or performance, unless the material or performance is sold, disseminated, displayed, possessed, controlled, brought or caused to be brought into this state, or presented for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial, or other proper purpose, by or to a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or research, librarian, clergyman, prosecutor, judge, or other person having a proper interest in the material or performance;

(3) Possess or view any material or performance that shows a minor who is not the person's child or ward in a state of nudity, unless one of the following applies:

(a) The material or performance is sold, disseminated, displayed, possessed, controlled, brought or caused to be brought into this state, or presented for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial, or other proper purpose, by or to a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or research, librarian, clergyman, prosecutor, judge, or other person having a proper interest in the material or performance.

(b) The person knows that the parents, guardian, or custodian has consented in writing to the photographing or use of the minor in a state of nudity and to the manner in which the material or performance is used or transferred.

(B) Whoever violates this section is guilty of illegal use of a minor in a nudity-oriented material or performance. Whoever violates division (A)(1) or (2) of this section is guilty of a felony of the second degree. Whoever violates division (A)(3) of this section is guilty of a misdemeanor of the first degree. If the offender previously has been convicted of or pleaded guilty to a violation of division (A)(3) of this section, illegal use of a minor in a nudity-oriented material or performance is a felony of the fourth degree.

HISTORY: 140 v H 44 (Eff 9-27-84); 140 v S 20[illegible]. Eff 4-9-85.

IN THE COMMON PLEAS COURT OF GREENE COUNTY, OHIO

FILED

1985 NOV 30 PM 3:34

STATE OF OHIO — CASE NO. 85 CR 23/24

Plaintiff

[illegible] CHRISTMAN CLERK
COMMON PLEAS COURT
GREENE COUNTY

-vs-

GEORGE and LINDA ROBINSON — JUDGMENT ENTRY

Defendants

This matter comes before the Court upon Defendants' Motion to Dismiss the Indictment on the grounds that O.R.C. Section 2907.323 and 2919.22(B)(4) are unconstitutional in that said statutes are vague, overbroad and violate Defendants' right of privacy.

Overbreadth and vagueness are two closely related doctrines important in dealing with free speech issues. Because of the importance of free speech in our society, even when the State has the power to regulate in an area, the power "must be so exercised as not, in obtaining a permissible end, to unduly infringe upon protected freedoms." Cantwell v. Connecticut, 310 U.S. 296, 304 (1940). Thus, an overbroad statute is one designed to punish activities which are not constitutionally protected, but the statute includes within its scope activities which are protected by the first amendment. In the case of a statute which is overbroad on its face, the Defendants' actions or speech may not be protected by the first amendment, and thus the act could have been prohibited under a carefully drawn statute. Nevertheless, the Court will strike an overbroad statute because it might apply to others not before the Court who may engage in a protected activity, which the statute appears to outlaw. People v. Holder, 103 Ill. App. 3d 353 at 356, 431 N.E. 2d 427, 430 (1982). As Justice Brennan explained in NAACP v. Burton, 371 U.S. 415, 432 (1963),

> "the instant decree may be invalid if it prohibits privileged exercise of first amendment rights whether or not the record discloses that the petitioner has engaged in privileged conduct. For in appraising a statute's inhibitory effect upon such rights, this court has not hesitated to take into account possible applications of the statute in other factual contexts beside that at bar."

In first amendment overbreadth cases, a statute will fail only if it is substantially overbroad and not readily reconstructed to avoid privileged activity. If it is not substantially overbroad it

is unlikely to have a drastic inhibitatory impact. As Justice White stated in Broderick v. Oklahoma, 413 U.S. 601, at 615 (1973),

> ". . . to put the matter another way, particularly where conduct and not merely speech is involved, we believe that the overbreadth of a statute must not only be real but substantial as well, judged in relation to the statute's substantial legitimate sweep."

Vague statutes suffer from three infirmities: 1) they fail to provide notice that the contemplated conduct is prohibited; 2) the guidelines are not reasonably clear which results in arbitrary and unequal enforcement and 3) the criminal statutes often proscribe conduct that is normally innocent. State v. Sammons, 58 Ohio St. 2d 460 (1979).

In order to prevent arbitrary enforcement under a vagueness analysis, a legislature is required to establish minimal guidelines to govern law enforcement in enforcing the statute. Kolander v. Lawson, 461 U.S. 352 (1983), Smith v. Goguen, 415 U.S. 556 (1974).

Thus, to survive a substantial overbreadth and vagueness challenge, a statute must be narrowly tailored to serve a compelling state interest. Maryland v. Joseph H. Munson Co. Inc., 468 U.S. (1984).

O.R.C. 2907.323 reads as follows:

> (A) No person shall do any of the following:
>
> (1) Photograph any minor who is not the person's child or ward in a state of nudity, or create, direct, produce, or transfer any material or performance that shows the minor in a state of nudity, unless both of the following apply:
>
> (a) The material or performance is, or is to be, sold, disseminated, displayed, possessed, controlled, brought or caused to be brought into this state, or presented for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial, or other proper purpose, by or to a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or research, librarian, clergyman, prosecutor, judge, or other person having a proper interest in the material or performance;
>
> (b) The minor's parents, guardian, or custodian consents in writing to the photographing of the minor, to the use of the minor in the material or performance, or to the transfer of the material and to the specific manner in which the material or performance is to be used.
>
> (2) Consent to the photographing of his minor child or ward, or photograph his minor child or ward, in a state of nudity or consent to the use of his minor child or ward in a state of nudity in any material or performance, or use or transfer such material or performance, unless the material or performance is sold, disseminated, displayed, possessed, controlled, brought or caused to be brought into this state, or presented for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial, or other proper purpose, by or to a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or

research, librarian, clergyman, prosecutor, judge, or other person having a proper interest in the material or performance;

(3) Possess or view any material or performance that shows a minor who is not the person's child or ward in a state of nudity, unless one of the following applies:

(a) The material or performance is sold, disseminated, displayed, possessed, controlled, brought or caused to be brought into this state, or presented for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial, or other proper purpose, by or to a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or research, librarian, clergyman, prosecutor, judge, or other person having a proper interest in the material or performance.

(b) The person knows that the parents, guardian, or custodian has consented in writing to the photographing or use of the minor in a state of nudity and to the manner in which the material or performance is used or transferred.

(B) Whoever violates this section is guilty of illegal use of a minor in a nudity-oriented material or performance. Whoever violates division (A)(1) or (2) of this section is guilty of a felony of the second degree. Whoever violates division (A)(3) of this section is guilty of misdemeanor of the first degree. If the offender previously has been convicted of or pleaded guilty to a violation of division (A)(3) of this section, illegal use of a minor in a nudity-oriented material or performance is a felony of the fourth degree.

In the case at bar, under O.R.C. Section 2907.323(A)(1), it is illegal to photograph a minor child who is not the person's child or ward in a state of nudity. A state may not ban nudity entirely, as to do so would be to equate nudity with obscenity. Erzhoznik v. Jacksonville, 422 U.S. 205 (1975). Clearly all nudity cannot be deemed obscene, even as to minors. Nor can such a broad restriction be justified by any governmental restriction pertaining to minors. Speech that is neither obscene as to minors nor subject to some other legitimate proscription cannot be suppressed solely because the legislative body finds such speech unsuitable. Erznoznik. The state, especially in the area of child pornography, may include materials that don't fit the definition of obscene under the Miller Test. New York v. Ferber, 458 U.S. 747 (1982). However, for a statute covering non-obscene material of child pornography to be valid, the forbidden acts depicted must be listed with sufficient precision and represent the kind of conduct or acts that lead to the sexual exploitation of the child. ORC 2901.323(A)(1) fails to be so narrowly tailored so as to sufficiently describe what type of conduct is illegal. Furthermore, the attempt to limit the scope of 2907.323(A)(1) is not in terms of what is illegal, but rather what conduct is legal.

This court notes that there are many situations which do not fit any of the specifically enumerated categories of 2907.323(A)(1)(a)&(b), yet the conduct is not illegal, but rather protected by the first amendment. A perfect example would be the case of a grandfather who takes a picture of his toddler grandchild in the tub. The grandfather would be held criminally liable, as the minor, who is not his child, is in a state of nudity; nor does this example fall within one of the enumerated categories.

Section 2907.323(A)(2) basically applies the same criteria to one's own child be it consent or actually photographing. Besides the above grandfather example and couples taking pictures of their naked child on the bearskin rug, Section (2) fails to address other various lifestyles - i.e., nudism. People who are nudists are expressing a belief. Nudity, without more, is a protected expression. Furthermore, one is given to expect certain privacy rights in one's own home. ORC 2907.323(A)(2) is extremely ripe for arbitrary enforcement - to enforce such an intrusive inquiry by the state into one's home life would deprive one of their privacy.

Section 2907.323(A)(3) suffers from the same basic defects as (1)&(2), but to a greater extent. It makes the mere possession or viewing of a photograph of a nude child (not their own) a crime. So grandpa, the neighbors or other relatives who just happen to view the photo are criminally liable.

Even assuming arguendo that the pictures are obscene, there is an even greater problem with the statute. This law would violate existing U.S. Supreme Court precedent. In Stanley v. Georgia, 394 U.S. 557 (1969), the court held that mere private possession of obscene material is not a crime. While the states generally retain broad power to regulate obscenity, that power does not extend to mere possession by an individual in the privacy of his own home. This is because the court in other contexts has been concerned with the sanctity of the home. Griswold v. Connecticut, 381 U.S. 479 (1965).

It should be noted in passing that a state may regulate non-obscene material in order to protect children from sexual expectation; but this is only applicable to cases where the state is seeking to enjoin the distribution of child pornography. New York vs. Ferber. This is because the distribution of child porn holds little First Amendment value - it is at best de minimus and there are no

constitutional considerations such as privacy to be asserted on the part of the child pornography vendor. Furthermore, the attempts of the legislature to limit the scope of the statute under 2907.323(A)(1)(a)&(b) and (3)(a)&(b) are poorly drafted. It doesn't state what is prohibited conduct as required by Ferber, but rather states what isn't prohibited. There are many situations in which conduct, while not obscene, does not fit the criteria set forth in the statute. This state should have specifically delineated the prohibited conduct to a reasonable degree.

Since the statute has such a sweeping meaning as to its terms, and the scope of its liability is unprecedented, said statute must be struck down as substantially overbroad and not narrowly drafted to serve compelling state interests. Therefore, it is ordered that Counts I, III, IV and VI of the indictment be dismissed.

In regard to Counts II and V charging both defendants with a violation of O.R.C. 2919.22(B)(4), the Court finds that the indictment and the Bill of Particulars taken together do not state an offense under Section 2919.22(B)(4). Section 2919.22(B)(4) is directed at "the production, presentation, dissemination, or advertisement of any material or performance. . . ." The prosecution in its Bill of Particulars does not charge the defendants with producing, presenting, disseminating, or advertising any material or performance that is obscene, or any material or performance that is sexually oriented or nudity-oriented matter. As such, the defendants' conduct as set out in the Bill of Particulars does not constitute a crime. The Ohio statute is of the same nature of the statute in Ferber. In that case the Supreme Court held that a state may prohibit the material or performance, even if it is not obscene, but only when it is aimed at distribution. For the above reasons stated herein, Counts II & V of the indictment are also dismissed.

SO ORDERED.

Exceptions noted.

JUDGE M. DAVID REID

AMERICAN COUNCIL ON EDUCATION

Division of Governmental Relations

November 8, 1985

The Honorable Paul Laxalt
Subcommittee on Criminal Law
Committee on the Judiciary
United States Senate
148 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Mr. Chairman:

On behalf of the American Council on Education, an organization representing over 1500 colleges and universities and the associations listed below, we wish to state our support for S. 440, the Computer Systems Protection Act, which would protect computers by criminalizing unauthorized access and fraudulent use or theft of computer information systems. Current legislation merely protects computers of the Federal Government, a good start in encouraging control of unauthorized computer-related actions. However, academic institutions remain unprotected by any federal computer crime legislation.

With this legislation in place, prosecutors would have a reasonable basis for instituting charges against anyone who steals, alters or destroys information in a computer or who makes an unauthorized entry into the system. An American Bar Association survey revealed that computer crime effected 50% of businesses last year and that three quarters of the crime occurred in-house. Survey data also showed that less than one third of computer theft and fraud was reported and another third was only "sometimes" reported.

A statute covering computer crime in interstate commerce would fill the interstices of other federal statutes which have failed to provide adequate protection and could also establish a pattern for states that have failed to enact computer fraud legislation.

The higher education community is increasingly dependent on computers both in terms of their use for research and for conducting business operations. Individuals are currently able to enter a system over telephone lines. As a result, information can be amended or deleted from various files contained within computer systems and the system itself caused to crash. Instances along the lines of the "War Games" model continue to occur on college campuses as students attempt to alter grades and unauthorized individuals gain access to privileged files. We support bills which would criminalize unauthorized access and are prepared to work with you and your staff to secure passage of such legislation in this session of Congress. If you have any questions relating to our position on this legislation, please do not hesitate to contact us.

One Dupont Circle, Washington, D.C. 20036-1193 (202) 939-9355

This letter is being sent on behalf of:

American Association of Community and Junior Colleges
American Association of State Colleges and Universities
American Council on Education
Association of American Universities
Association of Catholic Colleges and Universities
Association of Jesuit Colleges and Universities
Association of Urban Universities
Council of Independent Colleges
National Association of College and University Business Officers
National Association of Independent Colleges and Universities
National Association of Schools and Colleges of the United Methodist Church
National Association of State Universities and Land-Grant Colleges

Very truly yours,

Sheldon Elliot Steinbach
General Counsel

cc: Members of Committee

SES:mmb

Associated Credit Bureaus, Inc.

STATEMENT OF WALTER R. KURTH

PRESIDENT OF ASSOCIATED CREDIT BUREAUS, INC.

ON

S. 440 "The Computer Systems Protection Act";

S. 1678 "The Federal Computer Systems Protection Act of 1985";

and Other Computer Crime Legislation

On behalf of the 1,400 members of Associated Credit Bureaus, Inc. (ACB), an international trade association founded in 1906 to represent the consumer credit reporting industry, we are pleased to submit for the record the following statement to the Senate Judiciary Subcommittee on Criminal Law as it deliberates S. 440, S. 1678 and other computer crime legislation. While computer security remains a primary and integral part of the management effort of automated credit bureaus, computer vulnerabilities, both real and imagined, provide the basis for ongoing Congressional efforts to protect information resources.

Before proceeding with our comments, we would first like to applaud the actions of the Chairman whose efforts last year resulted in the inclusion of the Federal computer crime language in Public Law 98-473.

Last year, with ACB's support, Congress enacted legislation specifically making it a federal offense to access a consumer credit bureau computer without authorization. Specifically, Section 1030 (a) (2) of the Comprehensive Crime Control Act of 1984 (Public Law 98-473) states:

> "whoever knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such

authorization does not extend, and thereby obtains information...contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C.1681 et seq.)" shall be subject to the following maximum penalties:

First offense: a fine of $5000 or twice the value or loss created by the offense, and imprisonment for one (1) year;

Second offense: a fine of $10,000 or twice the value obtained or loss created by the offense, and imprisonment for ten (10) years.

For the reasons discussed below, we believe that the legislation enacted last year has made great strides towards preserving the integrity of consumers' credit histories, and therefore, we strongly oppose the provisions in S. 1678 which would repeal existing Section 1030 (a)(2) and replace it with more general language.

- The Fair Credit Reporting Act was enacted by Congress in recognition of the interstate nature of the industry to restrict the dissemination of information contained in a file maintained by a consumer reporting bureau relating to an individual's credit history. Existing Section 1030 has provided the credit bureau industry with an excellent tool to further enhance Congressional intent in enacting the Fair Credit Reporting Act. Therefore, to repeal Section 1030 would be taking a major step backward.

- ACB supports Congressional efforts to safeguard other types of equally sensitive and confidential information. However, Congress should not repeal the protection it has provided credit bureaus and consumers because it has not enacted legislation to protect other types of confidential information.

- The law is working, it is providing credit bureau management with an effective tool to be used in the hiring of credit bureau personnel and the selling of information within the intent of the Fair Credit Reporting Act.

- The credit reporting industry protections in the law are equally as important to credit granters, banks, retailers etc. because a primary reason to tamper with a credit bureau computer is to access records in order to obtain credit information and subsequently defraud credit granters.

- S. 1678 instead of tightening the law would create loopholes enabling criminals "hacking" credit bureau files to escape prosecution.

While ACB remains firm in its support for the retention of the provisions in existing Section 1030 providing protection to computers owned and operated by consumer reporting agencies, it is also our view that the stiffer criminal penalties contemplated in S. 440, S. 1677 and S. 1678 will go a long way in further deterring "hackers" from committing computer crimes.

As the Subcommittee knows, there has been a tendency on the part of the public to view computer crime as a form of intellectual pranksterism. Because of this inaccurate perception, societal definitions, deterrants and punishments are needed to control these white-collar crimes. The enactment of stronger criminal penalties will send a clear signal to those perpetrating computer crimes that there is as much wrongdoing in taking or abusing information contained in computers as there is in mugging a little old lady and taking her pocketbook. Therefore, ACB supports the strengthened criminal penalty provisions of S. 440, S. 1667 and S. 1678 as potential legislative vehicles for the further deterrence of computer crimes. However, we strongly believe that any federal computer crime legislation passed by the Congress must continue to make it a crime to illegally access a consumer reporting agency computer.

Crime has moved into the computer age and we support Congressional efforts to respond accordingly. ACB wishes to express its appreciation to the Subcommittee for the opportunity to submit this statement for the record and would be pleased to respond to any questions the Subcommittee may have.

○